TAMPEREEN YLIOPISTO

Pro gradu -tutkielma

Tytti Käyhkö

Neliökunnat

Informaatiotieteiden yksikkö

Matematiikka

Marraskuu 2016

Tampereen yliopisto

Informaatiotieteiden yksikkö

KÄYHKÖ, TYTTI: Neliökunnat

Pro gradu -tutkielma, 53 s.

Matematiikka

Marraskuu 2016

Tiivistelmä

Tässä tutkielmassa esitellään neliökunnan käsite ja siihen liittyviä tuloksia. Laajennetaan tavallisten kokonaislukujen joukkoa, jolloin saadaan neliökunnan kokonaisluvut. Tarkastellaan neliökuntien lukujen jaollisuutta, ja erityisesti tutustutaan alkulukuihin ja faktoriaalisuuteen sekä määritellään Eukleideen kunnan käsite. Lopuksi sovelletaan saatuja tuloksia kahteen eri Diofantoksen yhtälöön.

Päälähdeteoksena on käytetty Harold M. Starkin teosta An Introduction to Number Theory.

Sisältö

1 Johdanto

Tässä pro gradu -tutkielmassa tutustutaan neliökunnan käsitteeseen. Neliökunta $\mathbb{Q}(\sqrt{d})$ on rationaalilukujen kunnan laajennus, jonka alkiot ovat muotoa $a+b\sqrt{d}$, missä luvut a ja b ovat mielivaltaisia rationaalilukuja. Tutkielmassa oletetaan jotkin lukuteorian perustulokset tunnetuiksi ja niiden todistukset sivuutetaan.

Luvussa 2 määritellään tarkemmin neliökunta, ja tarkastellaan millaisia alkioita se sisältää. Luvun alussa todistetaan neliökunnan olevan suljettu peruslaskutoimituksien suhteen, eli alkioiden summa, erotus, tulo ja osamäärä kuuluvat neliökuntaan. Tämän jälkeen määritellään käsitteet liittoluku ja normi, sekä tutustutaan tarkemmin niiden ominaisuuksiin neliökunnassa. Luvun lopussa tutustutaan neliökunnan kokonaislukuihin ja huomataan sen olevan tavallisten kokonaislukujen joukon laajennus.

Luvussa 3 tarkastellaan kokonaislukujen jaollisuutta neliökunnissa. Määritellään siihen liittyviä tärkeitä käsitteitä, kuten yksikkö, alkuluku ja liitännäisluku. Esitellään yksiköiden perusominaisuuksia ja tarkastellaan yksiköiden määriä eri tapauksissa.

Luvussa 4 pääosassa ovat käsitteet faktoriaalinen rengas ja Eukleideen alue. Luvun lopussa esitellään kaikki mahdolliset neliökunnat, jotka ovat Eukleideen kuntia. Samoin kerrotaan, mitkä kompleksiset neliökunnat ($d < 0$) ovat faktoriaalisia renkaita. Reaalisten neliökuntien ($d > 0$) tapauksessa ongelma on edelleen avoin, joten tutustutaan vain muutamiin tunnettuihin tapauksiin. Näiden lauseiden todistukset sivuutetaan.

Luvussa 5 sovelletaan tuloksia kahteen eri Diofantoksen yhtälöön. Luvun alussa etsitään neliökunnan $\mathbb{Q}(\sqrt{-1})$ avulla Diofantoksen yhtälön $y^2 + 4 = z^3$ kokonaislukuratkaisut. Luvun lopussa esitellään tulos, jonka avulla nähdään onko Diofantoksen yhtälöllä $x^2 + y^2 = n$, missä $n \in \mathbb{Z}$, kokonaislukuratkaisuja.

Päälähdeteoksena on käytetty Harold M. Starkin teosta An Introduction to Number Theory.

2 Neliökunnat ja neliökokonaisluvut

Määritelmä 2.1. (ks. [4, s. 258]) Olkoon $d \in \mathbb{Q}$ sellainen luku, joka ei ole minkään rationaaliluvun neliö. Merkitään $\mathbb{Q}(\sqrt{d}) = a + b\sqrt{d}$, missä a ja b ovat mielivaltaisia rationaalilukuja. Kutsutaan joukkoa $\mathbb{Q}(\sqrt{d})$ varustettuna tavallisilla yhteen- ja kertolaskulla *neliökunnaksi*. Jos $d > 0$, kutsutaan joukkoa *reaalineliökunnaksi*, ja jos $d < 0$, kutsutaan joukkoa *kompleksiseksi* tai *imaginääriseksi neliökunnaksi*.

Esimerkki 2.1. $3 = 3 + 0\sqrt{2}$, $\frac{2}{3} + \frac{9}{7}\sqrt{2}$ ja $\sqrt{8} = 0 + 2\sqrt{2}$ ovat joukon $\mathbb{Q}(\sqrt{2})$ alkioita.

Koska jokainen rationaaliluku a voidaan kirjoittaa muodossa $a + 0\sqrt{d}$, niin voidaan todeta, että $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d})$. Jos luku d itse olisi jonkin rationaaliluvun neliö, niin $a + b\sqrt{d}$ olisi rationaalinen, jolloin $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$. Tästä syystä neliökunnan määritelmästä on poistettu tapaukset, joissa d on jonkin rationaaliluvun neliö, koska näistä tapauksista ei saada mitään uutta.

Jatkossa käytetään (mahdollisia poikkeuksia lukuunottamatta) pieniä roomalaisia kirjaimia a, b, c vastaamaan rationaalilukuja ja neliökunnan alkioita merkitään pienillä kreikkalaisilla kirjaimilla α, β, γ, δ,... . Kirjain d on varattu pelkästään sellaisen rationaaliluvun käyttöön, jossa $\sqrt{d}$ ei ole rationaalinen.

Lause 2.1. *Olkoot $a, b, c, e \in \mathbb{Z}$. Tällöin $a + b\sqrt{d} = c + e\sqrt{d}$, jos ja vain jos $a = c$ ja $b = e$. Erityisesti $a + b\sqrt{d} = 0$, jos ja vain jos $a = b = 0$.*

Todistus. (vrt. [4, s. 259]) Oletetaan ensin, että $a + b\sqrt{d} = 0$. Nythän $-a = b\sqrt{d}$. Jos $b \neq 0$, niin $\frac{-a}{b} = \sqrt{d}$, eli $\sqrt{d} \in \mathbb{Q}$, mikä on ristiriidassa oletuksen kanssa. On siis oltava $b = 0$, josta seuraa, että $a = 0$. Kääntäen, jos $a = b = 0$, niin $a + b\sqrt{d} = 0$.

Tarkastellaan nyt yleistä tapausta. Jos

$$a + b\sqrt{d} = c + e\sqrt{d},$$

niin

$$(a - c) + (b - e)\sqrt{d} = 0,$$

missä $a - c$, $b - e \in \mathbb{Q}$. Aiemman tapauksen nojalla on siis oltava $a - c = 0$ ja $b - e = 0$ eli $a = c$ ja $b = e$. Kääntäen, jos $a = c$ ja $b = e$, niin nähdään triviaalisti, että $a + b\sqrt{d} = c + e\sqrt{d}$. □

Huomautus. Edellisen lauseen väite ei toimi, mikäli $\sqrt{d} \in \mathbb{Q}$ tai mikäli lukuja a, b, c ja e ei ole rajoitettu olemaan joukossa $\mathbb{Q}$.

Todistus. Tarkastellaan tapausta $d = 1$, jolloin $\sqrt{d} = \sqrt{1} = 1 \in \mathbb{Q}$. Nyt saadaan $a + b = c + e$, ja esimerkiksi $3 + 4 = 1 + 6$, missä luvut $1, 3, 4, 6 \in \mathbb{Q}$, mutta $3 \neq 1$ ja $4 \neq 6$.

Tarkastellaan sitten tapausta, missä lukuja a, b, c, e ei ole rajoitettu joukkoon $\mathbb{Q}$. Olkoon $d = 2$. Kun valitaan $a = \sqrt{2}$, $b = \frac{1}{\sqrt{2}}$, $c = 1$ ja $e = 1$, niin

$$a + b\sqrt{2} = \sqrt{2} + \frac{1}{\sqrt{2}} = 1 + \sqrt{2} = c + e\sqrt{2},$$

mutta $a = \sqrt{2} \neq 1 = c$ ja $b = \frac{1}{\sqrt{2}} \neq 1 = e$. □

Lause 2.2. *Jos* $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$, *niin* $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta \in \mathbb{Q}(\sqrt{d})$. *Jos* $\beta \neq 0$, *niin* $\alpha/\beta \in \mathbb{Q}(\sqrt{d})$.

Todistus. (ks. [4, s. 259]) Merkitään $\alpha = a + b\sqrt{d}$ ja $\beta = c + e\sqrt{d}$, missä a, b, c, $e \in \mathbb{Q}$. Nyt

$$\begin{aligned} \alpha + \beta &= (a + c) + (b + e)\sqrt{d} \\ \alpha - \beta &= (a - c) + (b - e)\sqrt{d} \\ \alpha\beta &= (ac + bed) + (ae + bc)\sqrt{d} \end{aligned}$$

kuuluvat kaikki joukkoon $\mathbb{Q}(\sqrt{d})$, koska $(a+c)$, $(b+e)$, $(a-c)$, $(b-e)$, $(ae+bed)$, $(ae + bc) \in \mathbb{Q}$. Lisäksi, jos $\beta \neq 0$, niin $c \neq 0$ tai $e \neq 0$, joten $c - e\sqrt{d} \neq 0$. Siis

$$c^2 - e^2 d = (c + e\sqrt{d})(c - e\sqrt{d}) \neq 0,$$

koska kumpikaan tekijöistä ei ole nolla. Myös

$$\frac{\alpha}{\beta} = \frac{(a + b\sqrt{d})(c - e\sqrt{d})}{(c + e\sqrt{d})(c - e\sqrt{d})} = \left(\frac{ac - bed}{c^2 - e^2 d}\right) + \left(\frac{bc - ae}{c^2 - e^2 d}\right)\sqrt{d} \in \mathbb{Q}(\sqrt{d}),$$

koska luvut

$$\left(\frac{ac - bed}{c^2 - e^2 d}\right), \left(\frac{bc - ae}{c^2 - e^2 d}\right)$$

ovat rationaalilukujen osamääriä, joissa nimittäjä ei mene nollaksi, ja näin ollen rationaalisia. □

Tähän asti luku $d \in \mathbb{Q}$ on ollut sellainen, että $\sqrt{d} \notin \mathbb{Q}$. Voidaan kuitenkin rajoittaa lukua d vielä pidemmälle menettämättä yhtään neliökuntaa. Esimerkiksi

$$a + b\sqrt{\frac{2}{3}} = a + \left(\frac{b}{3}\right)\sqrt{6},$$

joten $\mathbb{Q}(\sqrt{\frac{2}{3}}) = \mathbb{Q}(\sqrt{6})$. Siis joukot $\mathbb{Q}(\sqrt{\frac{2}{3}})$, $\mathbb{Q}(\sqrt{6})$ sisältävät täsmälleen samat luvut. Yleisemmin

$$\mathbb{Q}\left(\sqrt{\frac{r}{s}}\right) = \mathbb{Q}(\sqrt{rs}),$$

koska $a + b\sqrt{\frac{r}{s}} = a + b\left(\frac{\sqrt{r}}{\sqrt{s}}\right) = a + b\left(\frac{\sqrt{r}\sqrt{s}}{s}\right) = a + \frac{b}{s}(\sqrt{r}\sqrt{s}) = a + \frac{b}{s}\sqrt{rs}$, missä luvut $r, s \in \mathbb{Z}$, $s \neq 0$ ja $rs \in \mathbb{Z}$. Riittää siis tarkastella luvun d kokonaislukuarvoja. Huomataan, että lukua d voidaan edelleen rajoittaa. Esimerkiksi

$$a + b\sqrt{8} = a + (2b)\sqrt{2},$$

joten $\mathbb{Q}(\sqrt{8}) = \mathbb{Q}(\sqrt{2})$. Yleisesti voidaan kirjoittaa $\mathbb{Q}(\sqrt{r^2 s}) = \mathbb{Q}(\sqrt{s})$. Täten tarvitsee tarkastella vain luvun d kokonaislukuarvoja, joilla ei ole neliötekijöitä ($\neq 1$). Tällaisen luvun sanotaan olevan *neliövapaa*. Tästä eteenpäin d on kiinnitetty kokonaisluku, missä $d \neq 0$, $d \neq 1$ ja luvulla d ei ole neliötekijöitä ($\neq 1$). Koska $d \neq 0$ tai 1, eikä luvulla d ole neliötekijöitä, niin d ei ole täydellinen neliö, ja siten $\sqrt{d}$ on irrationaalinen. Ensimmäiset hyväksyttävät positiiviset arvot, jotka kelpaavat luvuksi d ovat 2, 3, 5, 6, 7, 10, 11,... Vastaavasti ensimmäiset hyväksyttävät negatiiviset arvot luvulle d ovat $-1, -2, -3, -5, -6, -7, -10, -11$,...

Joukon $\mathbb{Q}(\sqrt{d})$ alkiot ovat toisen asteen kokonaislukukertoimisen yhtälön ratkaisuja. Huomataan, että luku $a + b\sqrt{d}$ on rationaalikertoimisen yhtälön

$$x^2 - ax + (a^2 - b^2 d) = [x - (a + b\sqrt{d})][x - (a - b\sqrt{d})] = 0$$

ratkaisu. Jos kerrotaan yhtälö puolittain yhteisellä nimittäjällä, niin saadaan toisen asteen yhtälö, jolla on kokonaislukukertoimet. Tämän yhtälön kaksi ratkaisua ovat luvut $a + b\sqrt{d}$ ja $a - b\sqrt{d}$, jotka ovat toistensa liittolukuja.

Määritelmä 2.2. (ks. [4, s. 261]) Jos $\alpha = a + b\sqrt{d}$, niin luvun α *liittoluku* on $\overline{\alpha} = a - b\sqrt{d}$.

Jos $d < 0$, niin määritelmä on tuttu tavallisen kompleksiluvun kompleksiliittoluvun määritelmästä.

Huomautus. $\mathbb{Q}(\sqrt{d})$ on tosiaan kunta, koska jos $0 \neq a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, niin sillä on käänteisalkio

$$\begin{aligned}\frac{1}{a+b\sqrt{d}} &= \frac{a-b\sqrt{d}}{(a-b\sqrt{d})(a+b\sqrt{d})} \\ &= \frac{a-b\sqrt{d}}{a^2-b^2d} \\ &= \frac{a}{a^2-b^2d} - \frac{b}{a^2-b^2d}\sqrt{d},\end{aligned}$$

missä $\frac{a}{a^2-b^2d}, \frac{b}{a^2-b^2d}\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ ja $a^2 - b^2d \neq 0$, koska d ei ole neliö.

Lause 2.3. *Jos $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$, niin $\overline{(\overline{\alpha})} = \alpha$, $\overline{(\alpha+\beta)} = \overline{\alpha} + \overline{\beta}$, $\overline{(\alpha-\beta)} = \overline{\alpha} - \overline{\beta}$, $\overline{(\alpha\beta)} = \overline{\alpha}\overline{\beta}$. Jos lisäksi $\beta \neq 0$, niin $\overline{\beta} \neq 0$ ja $\overline{(\alpha/\beta)} = \overline{\alpha}/\overline{\beta}$. Edelleen $\overline{\alpha} = \alpha$, jos ja vain jos $\alpha \in \mathbb{Q}$.*

Todistus. (vrt. [4, s. 261]) Olkoot $\alpha = a + b\sqrt{d}$, $\beta = c + e\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. Nyt

$$\begin{aligned}\overline{(\overline{\alpha})} &= \overline{(a-b\sqrt{d})} = a + b\sqrt{d} = \alpha \\ \overline{(\alpha+\beta)} &= \overline{[(a+c)+(b+e)\sqrt{d}]} = (a+c)-(b+e)\sqrt{d} \\ &= (a-b\sqrt{d})+(c-e\sqrt{d}) = \overline{\alpha}+\overline{\beta} \\ \overline{(\alpha-\beta)} &= \overline{[(a-c)+(b-e)\sqrt{d}]} = (a-c)-(b-e)\sqrt{d} \\ &= (a-b\sqrt{d})-(c-e\sqrt{d}) = \overline{\alpha}-\overline{\beta} \\ \overline{(\alpha\beta)} &= \overline{[(ac+bed)+(ae+bc)\sqrt{d}]} = (ac+bed)-(ae+bc)\sqrt{d} \\ &= (a-b\sqrt{d})(c-e\sqrt{d}) = \overline{\alpha}\overline{\beta}.\end{aligned}$$

Jos $\alpha = \overline{\alpha}$, niin $a + b\sqrt{d} = a - b\sqrt{d}$. On siis oltava $b = -b$, eli $b = 0$, joten $\alpha = a$ on rationaalinen. Kääntäen, jos $\alpha = a + 0\sqrt{d} \in \mathbb{Q}$, niin $\overline{\alpha} = a - 0\sqrt{d} = \alpha$.

Lauseen alkuosan perusteella, jos $\beta \neq 0$, niin $c \neq 0$ tai $e \neq 0$, joten $\overline{\beta} = c - e\sqrt{d} \neq 0$. Koska $1/(\beta\overline{\beta}) = 1/(c^2 - e^2d) \in \mathbb{Q}$, niin

$$\overline{\left(\frac{\alpha}{\beta}\right)} = \overline{\left(1/(\beta\overline{\beta})\cdot\alpha\cdot\overline{\beta}\right)} = \overline{\left(1/(\beta\overline{\beta})\right)}\cdot\overline{\alpha}\cdot\overline{\left(\overline{\beta}\right)} = 1/(\beta\overline{\beta})\cdot\overline{\alpha}\cdot\beta = \overline{\alpha}/\overline{\beta}.$$

□

Oletetaan, että luku α on kokonaislukukertoimisen toisen asteen yhtälön

$$ax^2 + bx + c = 0$$

ratkaisu. Koska luku α toteuttaa tämän yhtälön ja koska luvut $a, b, c \in \mathbb{Q}$, niin

$$\begin{aligned} a(\overline{\alpha})^2 + b\overline{\alpha} + c &= \overline{a}(\overline{\alpha^2}) + \overline{b}\overline{\alpha} + \overline{c} = (\overline{a\alpha^2}) + (\overline{b\alpha}) + \overline{c} \\ &= (\overline{a\alpha^2 + b\alpha + c}) = (\overline{0}) = 0. \end{aligned}$$

Toisin sanoen, jos α on yhtälön $ax^2 + bx + c = 0$ ratkaisu, niin tällöin myös $\overline{\alpha}$ on yhtälön ratkaisu. Oletetaan, että α on irrationaalinen, jolloin $\alpha \neq \overline{\alpha}$. Tällöin yhtälölle on löydetty kaksi ratkaisua. Koska toisen asteen polynomi voidaan jakaa juurien mukaan tekijöihin, niin

$$ax^2 + bx + c = a(x - \alpha)(x - \overline{\alpha}).$$

Siis on olemassa äärettömän monta toisen asteen kokonaislukukertoimista yhtälöä, joiden ratkaisuna on α, mutta ne eroavat toisistaan vain vakion a verran. Jakamalla yhtälö $ax^2 + bx + c = 0$ lukujen a, b ja c suurimmalla yhteisellä tekijällä, ja tarvittaessa kertomalla luvulla -1, saadaan yksikäsitteinen toisen asteen yhtälö luvulle α.

Apulause 2.1. Olkoon $a \in \mathbb{Z}$ ja $n > 0$. Tällöin, jos $\sqrt[n]{a} \in \mathbb{Q}$, niin $\sqrt[n]{a} \in \mathbb{Z}$.

Todistus. (vrt. [2]) Oletetaan, että $\sqrt[n]{a} \in \mathbb{Q}$. Siis on olemassa sellaiset keskenään jaottomat $s, r \in \mathbb{Z}$, $r \neq 0$, että

$$\sqrt[n]{a} = \frac{s}{r}.$$

Näin ollen

$$\begin{aligned} a &= \left(\frac{s}{r}\right)^n \\ a &= \frac{s^n}{r^n} \\ ar^{n-1} &= \frac{s^n}{r}. \end{aligned}$$

Nyt $ar^{n-1} \in \mathbb{Z}$, joten myös $\frac{s^n}{r} \in \mathbb{Z}$. Koska $\text{syt}(s,r) = 1$, niin oltava $r = \pm 1$. Näin ollen $\sqrt[n]{a}$ on kokonaisluku. □

Huomautus. Edellisen apulauseen nojalla, jos $x^n \in \mathbb{Z}$ ja $x \in \mathbb{Q}$, niin $x \in \mathbb{Z}$.

Määritelmä 2.3. (ks. [4, s. 262]) Jos $\alpha \in \mathbb{Q}(\sqrt{d})$ on irrationaalinen, missä a, b, $c \in \mathbb{Z}$ ja $\text{syt}(a,b,c) = 1$, $a > 0$, niin yhtälöä $ax^2 + bx + c = 0$ kutsutaan luvun α *määrittteleväksi yhtälöksi*, mikäli α toteuttaa yhtälön.

Esimerkki 2.2. Esimerkiksi $2 + \sqrt{3}$ toteuttaa yhtälöt

$$-x^2 + 4x - 1 = 0,$$
$$3x^2 - 12x + 3 = 0,$$
$$-5x^2 + 20x - 5 = 0.$$

Kaikki nämä yhtälöt ovat monikertoja yhtälöstä $x^2 - 4x + 1 = 0$, jonka ratkaisu luku $2 + \sqrt{3}$ on.

Esimerkki 2.3. Irrationaalinen luku voi olla korkeintaan yhdessä neliökunnassa. Toisin sanoen kahden eri neliökunnan leikkaus on joukko $\mathbb{Q}$.

Todistus. (vrt. [4, s. 262]) Oletetaan, että irrationaalinen luku $\alpha \in \mathbb{Q}(\sqrt{d})$ ja $\alpha \in \mathbb{Q}(\sqrt{d_1})$. Nyt

$$\alpha = a + b\sqrt{d} = a_1 + b_1\sqrt{d_1},$$

missä $a, b, a_1, b_1 \in \mathbb{Q}$. Määrittelevän yhtälön toinen ratkaisu on α ja toinen on

$$\overline{\alpha} = a - b\sqrt{d} = a_1 - b_1\sqrt{d_1}.$$

Siis

$$b\sqrt{d} = \frac{\alpha - \overline{\alpha}}{2} = b_1\sqrt{d_1},$$

joten ($b \neq 0$, koska α on irrationaalinen)

$$\frac{b\sqrt{dd_1}}{\sqrt{d_1}} = b_1\sqrt{d_1},$$

mistä saadaan ratkaistua

$$\sqrt{dd_1} = \frac{b_1 d_1}{b}.$$

Täten $\sqrt{dd_1} \in \mathbb{Q}$, joten apulauseen 2.1 nojalla $\sqrt{dd_1} \in \mathbb{Z}$. Nythän d ja d_1 ovat neliövapaita ja dd_1 on täydellinen neliö. Alkutekijähajotelman yksikäsitteisyyslauseen nojalla luvuilla d ja d_1 on oltava sama merkki ja samat alkutekijät, joten $d = d_1$, kuten toivottiin. □

Määritelmä 2.4. (ks. [4, s. 263]) Luvun $\alpha \in \mathbb{Q}(\sqrt{d})$ *normi* on luku $\mathbf{N}(\alpha) := \alpha\overline{\alpha}$.

Lause 2.4. *Olkoot α, $\beta \in \mathbb{Q}(\sqrt{d})$.*

a) Jos $a \in \mathbb{Q}$, niin $\boldsymbol{N}(a) = a^2$.

b) $\boldsymbol{N}(\alpha) \in \mathbb{Q}$.

c) Jos $d < 0$, niin $\boldsymbol{N}(\alpha) \geq 0$. Erityisesti $\boldsymbol{N}(\alpha) = 0$, jos ja vain jos $\alpha = 0$.

d) $\boldsymbol{N}(\alpha\beta) = \boldsymbol{N}(\alpha)\boldsymbol{N}(\beta)$. Lisäksi, jos $\beta \neq 0$, niin

$$\boldsymbol{N}\left(\frac{\alpha}{\beta}\right) = \frac{\boldsymbol{N}(\alpha)}{\boldsymbol{N}(\beta)}.$$

Todistus. (vrt. [4, s. 263]) Merkitään $\alpha = a + b\sqrt{d}$, missä $a, b \in \mathbb{Q}$.

a) Koska luku $a \in \mathbb{Q}$, niin $\overline{a} = a$ ja siten $\mathbf{N}(a) = a\overline{a} = a^2$.

b) Huomataan, että

$$\mathbf{N}(\alpha) = \alpha\overline{\alpha} = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d = a^2 + (-d)b^2,$$

joka on rationaaliluku. Normin $\mathbf{N}(\alpha)$ rationaalisuus oltaisiin voitu osoittaa myös seuraavasti:

$$\overline{\mathbf{N}(\alpha)} = \overline{\alpha\overline{\alpha}} = \overline{\alpha}\alpha = \alpha\overline{\alpha} = \mathbf{N}(\alpha),$$

joten lauseen 2.3 perusteella normi $\mathbf{N}(\alpha)$ on rationaalinen.

c) Tapauksessa $d < 0$ pätee tietenkin $(-d) > 0$, joten $\mathbf{N}(\alpha) \geq 0$. Selvästi $\mathbf{N}(0) = 0$. Jos $\alpha \neq 0$, niin $\overline{\alpha} \neq 0$ ja siten $\mathbf{N}(\alpha) = \alpha\overline{\alpha} \neq 0$. Täten nähdään, että $\mathbf{N}(\alpha) = 0$, jos ja vain jos $\alpha = 0$.

d) Normin määritelmän ja lauseen 2.3 perusteella

$$\mathbf{N}(\alpha\beta) = (\alpha\beta)(\overline{\alpha\beta}) = \alpha\beta\overline{\alpha}\,\overline{\beta} = \mathbf{N}(\alpha)\mathbf{N}(\beta).$$

Jos $\beta \neq 0$, niin

$$\mathbf{N}\left(\frac{\alpha}{\beta}\right) = \left(\frac{\alpha}{\beta}\right)\left(\overline{\frac{\alpha}{\beta}}\right) = \frac{\alpha}{\beta} \cdot \frac{\overline{\alpha}}{\overline{\beta}} = \frac{\mathbf{N}(\alpha)}{\mathbf{N}(\beta)}.$$

□

Yllä oleva yhtälö $\mathbf{N}(\alpha)\mathbf{N}(\beta) = \mathbf{N}(\alpha\beta)$ voi vaikuttaa triviaalilta, mutta kun siihen sijoitetaan $\alpha = a + b\sqrt{d}$, $b = c + e\sqrt{d}$, niin saadaan

$$\begin{aligned}(a + b\sqrt{d})(a - b\sqrt{d})(c + e\sqrt{d})(c - e\sqrt{d}) &= (a^2 - db^2)(c^2 - de^2) \\ &= (ac + bed)^2 - d(ae + bc)^2.\end{aligned}$$

Tarkastellaan tapausta $d = -1$. Nythän, jos kaksi lukua voidaan kirjoittaa kahden neliön summana, niin tällöin myös niiden tulo on kahden neliön summa. Toisin sanoen

$$(a^2 + b^2)(c^2 + e^2) = (ac - be)^2 + (ae + bc)^2.$$

Siis yhtälöllä $\mathbf{N}(\alpha)\mathbf{N}(\beta) = \mathbf{N}(\alpha\beta)$ on enemmän sisältöä kuin aluksi vaikuttaa.

Seuraavaksi tarkastellaan kokonaislukuja $a + b\sqrt{d}$ joukossa $\mathbb{Q}(\sqrt{d})$. Koska neliökunta $\mathbb{Q}(\sqrt{d})$ sisältää muitakin kuin joukon $\mathbb{Q}$ alkioita, niin on järkevää määritellä joukkoon muitakin kuin pelkkiä tavallisia kokonaislukuja (tapaukset $a \in \mathbb{Z}$ ja $b = 0$).

Apulauseen 2.1 jälkeisen huomautuksen nojalla, jos $x^n \in \mathbb{Z}$ ja $x \in \mathbb{Q}$, niin $x \in \mathbb{Z}$. Halutaan laajentaa tämä ominaisuus myös joukkoon $\mathbb{Q}(\sqrt{d})$. Tästä syystä, kun d on kokonaisluku ja $\sqrt{d}$ on yhtälön $x^2 = d$ ratkaisu, niin määritellään luvun $\sqrt{d}$ olevan kokonaisluku. Halutaan kokonaislukujen summien ja tulojen olevan edelleen kokonaislukuja. Jos $a, b \in \mathbb{Z}$, niin toivotaan, että tulo $b\sqrt{d}$ ja summa $a + b\sqrt{d}$ ovat myös kokonaislukuja.

Tähän mennessä ollaan valittu kokonaisluvut määrittelevän yhtälön avulla. Esimerkiksi määrittelevä yhtälö luvulle $\sqrt{d}$ on $x^2 - d = 0$ ja määrittelevä yhtälö luvulle $(-\frac{1}{2}) + (\frac{1}{2})\sqrt{-3}$ on $x^2 + x + 1 = 0$. Näillä yhtälöillä yhteistä on se, että toisen asteen termin kerroin on yksi.

Määritelmä 2.5. (vrt. [4, s. 265]) Luku $\alpha \in \mathbb{Q}(\sqrt{d})$ on *(neliö)kokonaisluku*, jos joko $\alpha \in \mathbb{Z}$ tai luvun α määrittelevä yhtälö on muotoa $x^2 + ax + b = 0$, missä $a, b \in \mathbb{Z}$. Merkitään jatkossa (neliö)kokonaislukujen joukkoa symbolilla $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Voidaan käyttää myös merkintää $\mathcal{O}$, mikäli neliökunta on asiayhteydestä selvä. Joukon $\mathbb{Z}$ alkioita kutsutaan jatkossa *rationaalikokonaisluvuiksi*.

Huomautus. Merkintä $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ esiintyy useissa eri lähteissä, esimerkiksi [1], [3] ja [7].

Määritelmän 2.5 nojalla, jos neliökokonaisluku on rationaalinen, niin se on perinteinen kokonaisluku eli rationaalikokonaisluku. Ei olla siis esitelty uusia joukon $\mathbb{Q}$ kokonaislukuja. Huomataan myös, että määrittelevä yhtälö on sama luvuille α ja $\bar{\alpha}$.

Joukon $\mathbb{Q}(\sqrt{d})$ kokonaisluvut toteuttavat perinteiset laskutoimitukset, eli kahden kokonaisluvun summa, erotus ja tulo ovat edelleen kokonaislukuja.

Esimerkki 2.4. Luku $\frac{1+\sqrt{3}}{2}$ ei ole kokonaisluku joukossa $\mathbb{Q}(\sqrt{3})$.

Todistus. Etsitään luvun $\frac{1+\sqrt{3}}{2}$ määrittelevä yhtälö:

$$\begin{aligned}\left(x-\frac{1+\sqrt{3}}{2}\right)\left(x-\frac{1-\sqrt{3}}{2}\right) &= x^2-\left(\frac{1+\sqrt{3}}{2}\right)x-\left(\frac{1-\sqrt{3}}{2}\right)x-\left(\frac{1+\sqrt{3}}{2}\right)\left(\frac{1-\sqrt{3}}{2}\right)\\ &= 4x^2-2x-2\sqrt{3}x-2x+2\sqrt{3}x-2\\ &= 2x^2-2x-1.\end{aligned}$$

Koska luvun $\frac{1+\sqrt{3}}{2}$ määrittelevä yhtälö ei ole muotoa $x^2+ax+b=0$, niin luku $\frac{1+\sqrt{3}}{2}$ ei ole kokonaisluku joukossa $\mathbb{Q}(\sqrt{3})$. □

Esimerkki 2.5. Luku 10 on kokonaisluku joukossa $\mathbb{Q}(\sqrt{d})$, koska $10 \in \mathbb{Z}$.

Apulause 2.2. Jos $b \in \mathbb{Z}$ on pariton, niin $b^2 \equiv 1 \pmod 4$

Todistus. Olkoon $b \in \mathbb{Z}$ pariton. Tällöin voidaan kirjoittaa $b = 2m+1$, missä $m \in \mathbb{Z}$. Nyt

$$b^2 = (2m+1)^2 = 4m^2+4m+1 = 4(m^2+m)+1 \equiv 1 \pmod 4$$

□

Huomautus. Seuraavassa lauseessa tunnistetaan joukon $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ alkiot. Tapauksen $d \equiv 1 \pmod 4$ tarkempi tarkastelu tapahtuu lauseessa 2.6.

Lause 2.5. *a) Jos* $d \not\equiv 1 \pmod 4$, *niin* $\mathcal{O} = \left\{a+b\sqrt{d} \mid a,b \in \mathbb{Z}\right\} =: \mathbb{Z}[\sqrt{d}]$.

b) Jos $d \equiv 1 \pmod 4$, *niin*

$$\mathcal{O} = \left\{\frac{a+b\sqrt{d}}{2} \mid a,b \text{ parillisia}\right\} \cup \left\{\frac{a+b\sqrt{d}}{2} \mid a,b \text{ parittomia}\right\} =: \mathbb{Z}[\omega].$$

Todistus. (vrt. [4, s. 266]) Jaetaan todistus osiin seuraavasti:

1) Tapauksessa a) pätee $\mathcal{O} \supseteq \mathbb{Z}[\sqrt{d}]$

2) Tapauksessa b) pätee $\mathcal{O} \supseteq \mathbb{Z}[\omega]$

3) Kohtien 1) ja 2) osajoukkoudet ovat yhtäsuuruuksia

Todistetaan aluksi kohtien 1) ja 2) tapaus $b = 0$. Siis, jos $\alpha = a + b\sqrt{d}$, missä luvut a, $b \in \mathbb{Z}$, niin $\alpha \in \mathbb{Q}$, jos ja vain jos $b = 0$. Siten $\alpha \in \mathbb{Z}$, jos ja vain jos $a \in \mathbb{Z}$ ja $b = 0$, ja tällöin se on muotoa

$$\begin{aligned}\alpha &= a + b\sqrt{d} \qquad\qquad (a, b \in \mathbb{Z}, \text{ tapaus } d \not\equiv 1 \pmod 4)\\ &= \frac{2a + 2b\sqrt{d}}{2} \ (2a, 2b \text{ parillisia, tapaus d } \equiv 1 \pmod 4).\end{aligned}$$

Tästä eteenpäin todistuksessa oletetaan, että $\alpha = a + b\sqrt{d}$ on irrationaalinen eli $b \neq 0$.

1) Jos $\alpha = a + b\sqrt{d}$, missä a, $b \in \mathbb{Z}$, niin α toteuttaa yhtälön

$$\begin{aligned}(x - \alpha)(x - \bar{\alpha}) &= (x - (a + b\sqrt{d}))(x - (a - b\sqrt{d}))\\ &= x^2 - ax + b\sqrt{d}x - ax + a^2 - b\sqrt{d}a - b\sqrt{d}x + b\sqrt{d}a - b^2d\\ &= x^2 - 2ax + (a^2 - b^2d)\\ &= 0,\end{aligned}$$

missä $-2a$, $a^2 - b^2d \in \mathbb{Z}$. Tässä yhtälössä kertoimilla ei selvästikään ole muita yhteisiä tekijöitä kuin ± 1 (koska 1 on johtava kerroin), joten tämä on luvun α määrittelevä yhtälö. Siis α on kokonaisluku.

2) Oletetaan sitten, että $d \equiv 1 \pmod 4$ ja $\alpha = (a + b\sqrt{2})/2$, missä a ja b ovat parittomia joukossa $\mathbb{Z}$. (Tapaus, jossa luvut a ja b ovat parillisia, on jo todistettu kohdassa 1.) Tällöin α on yhtälön

$$\begin{aligned}(x - \alpha)(x - \bar{\alpha}) &= \left(x - \left(\frac{a + b\sqrt{2}}{2}\right)\right)\left(x - \left(\frac{a - b\sqrt{2}}{2}\right)\right)\\ &= x^2 - \frac{ax}{2} + \frac{b\sqrt{d}x}{2} - \frac{ax}{2} + \frac{a^2}{4} - \frac{b\sqrt{d}a}{4} - \frac{b\sqrt{d}x}{2} + \frac{b\sqrt{d}a}{4} + \frac{b^2d}{4}\\ &= x^2 - ax + \left(\frac{a^2 - b^2d}{4}\right)\\ &= 0\end{aligned}$$

ratkaisu. Osoitetaan, että $\frac{a^2 - b^2d}{4} \in \mathbb{Z}$. Merkitään $a = 2m + 1$ ja $b = 2n + 1$, missä n, $m \in \mathbb{Z}$. Nyt

$$\begin{aligned}\frac{a^2 - b^2d}{4} &= \frac{am^2 + 4m + 1 - (4n^2 + 4n + 1)d}{4}\\ &= \frac{4(m^2 - n^2d) + 4(m - nd) + 1 - d}{4}\\ &= (m^2 - n^2d) + (m - nd) + \frac{1 - d}{4},\end{aligned}$$

missä $m^2 - n^2 d$, $m - nd \in \mathbb{Z}$. Lisäksi

$$\begin{aligned} d &\equiv 1 \pmod 4 \\ \Rightarrow -d &\equiv -1 \pmod 4 \\ \Rightarrow 1 - d &\equiv 0 \pmod 4, \end{aligned}$$

joten $4 \mid 1 - d$, eli $\frac{1-d}{4} \in \mathbb{Z}$. Siis α on kokonaisluku.

3) Kääntäen, oletetaan, että α on irrationaalinen kokonaisluku joukossa $\mathcal{O}$. Siispä luvun α määrittelevä yhtälö on muotoa $x^2 + kx + l = 0$, missä $k, l \in \mathbb{Z}$. Tällöin k on parillinen tai pariton. Oletetaan ensin, että k on parillinen. Merkitään $k = 2m$, missä $m \in \mathbb{Z}$. Tällöin toisen asteen yhtälön ratkaisukaavan nojalla

$$\alpha = \frac{k \pm \sqrt{k^2 - 4l}}{2} = \frac{2m \pm \sqrt{4m^2 - 4l}}{2} = m \pm \sqrt{m^2 - l}.$$

Voidaan kirjoittaa $m^2 - l = e^2 d'$, missä e, $d' \in \mathbb{Z}$ ja d' on neliövapaa (ja d' ei ole 0 tai 1, koska α ei ole rationaalinen). Nyt α on toinen luvuista $-m \pm e\sqrt{d'} = (-2m \pm 2e\sqrt{d'})/2 \in \mathbb{Q}(\sqrt{d'})$, missä $-m, \pm e \in \mathbb{Z}$. Aiemmin on jo todettu (esimerkki 2.3), että $d = d_1$, joten α kuuluu haluttuun joukkoon luvun d jakojäännöksestä huolimatta.

Tarkastellaan seuraavaksi tapausta k on pariton. Tällöin

$$\alpha = \frac{-k \pm \sqrt{k^2 - 4l}}{2}.$$

Koska k on pariton, niin apulauseen 2.2 nojalla

$$k^2 - 4l \equiv 1 - 4l \equiv 1 \pmod 4.$$

Merkitään $k^2 - 4l = e^2 d'$, missä luvulla d' ei ole epätriviaaleja neliötekijöitä (ja $d' \notin \{0, 1\}$, koska α on irrationaalinen). Nyt e on pariton, koska $k^2 - 4l$ on pariton, ja siten

$$d' = 1 \cdot d' \equiv e^2 d' = k^2 - 4c \equiv 1 \pmod 4.$$

Koska α on toinen luvuista

$$\frac{-k \pm e\sqrt{d'}}{2},$$

niin α on joukon $\mathbb{Q}(\sqrt{d'})$ alkio, missä $d' \equiv 1 \pmod 4$, ja sekä $-k$ että $\pm e$ ovat parittomia. Tässäkin tapauksessa $d' = d$, joten α kuuluu haluttuun joukkoon

$$\left\{ \frac{a + b\sqrt{d}}{2} \mid a, b \text{ parillisia} \right\} \cup \left\{ \frac{a + b\sqrt{d}}{2} \mid a, b \text{ parittomia} \right\}.$$

□

Huomautus. Edellisestä lauseesta seuraa, että jos a, $b \in \mathbb{Z}$, niin $a + b\sqrt{d}$ on aina kokonaisluku, eli $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}$. Tapauksessa $d \not\equiv 1 \pmod 4$ tämä on triviaalia. Jos $d \equiv 1 \pmod 4$, niin luku $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ voidaan ilmaista muodossa $(2a + 2b\sqrt{d})/2$, missä molemmat $2a$ ja $2b$ ovat tietenkin parillisia, joten $a + b\sqrt{d} \in \mathcal{O}$.

Esimerkki 2.6. Luku $\frac{3+2\sqrt{6}}{1-\sqrt{6}}$ on kokonaisluku joukossa $\mathbb{Q}(\sqrt{6})$.

Todistus. Huomataan, että

$$\begin{aligned} \frac{3 + 2\sqrt{6}}{1 - \sqrt{6}} &= \frac{(1 + \sqrt{6})(3 + 2\sqrt{6})}{(1 + \sqrt{6})(1 - \sqrt{6})} \\ &= \frac{3 + 2\sqrt{6} + 3\sqrt{6} + 12}{1 - 6} \\ &= \frac{15 + 5\sqrt{6}}{-5} \\ &= -3 - \sqrt{6}, \end{aligned}$$

joten lauseen 2.5 mukaan $\frac{3+2\sqrt{6}}{1-\sqrt{6}}$ on kokonaisluku. □

Seuraus 2.1. Olkoon $d \equiv 1 \pmod 4$. Tällöin $\alpha \in \mathcal{O}$, jos ja vain jos

$$\alpha = a + b\left(\frac{1 + \sqrt{d}}{2}\right),$$

missä a, $b \in \mathbb{Z}$

Todistus. (vrt. [4, s. 266]) Oletetaan, että $\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right)$, missä a, $b \in \mathbb{Z}$. Tällöin

$$a + b\left(\frac{1 + \sqrt{d}}{2}\right) = \frac{(2a + b) + b\sqrt{d}}{2},$$

missä $2a + b \equiv b \pmod 2$, ja siten $(2a + b)$ ja b ovat molemmat joko parillisia ja parittomia. Siis $\alpha \in \mathcal{O}$.

Oletetaan sitten, että $\alpha \in \mathcal{O}$. Tällöin lauseen 2.5 nojalla $\alpha = \frac{a+b\sqrt{d}}{2}$, missä a, $b \in \mathbb{Z}$, ja missä molemmat ovat parillisia tai molemmat ovat parittomia, ja

$$\frac{a+b\sqrt{d}}{2} = \left(\frac{a-b}{2}\right) + b\left(\frac{1+\sqrt{d}}{2}\right),$$

Koska $a \equiv b \pmod 2$, niin $a - b \equiv 0 \pmod 2$, eli $(a-b)/2 \in \mathbb{Z}$. □

Lause 2.6. *Jos α, $\beta \in \mathcal{O}$, niin $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta \in \mathcal{O}$.*

Todistus. (vrt. [4, s. 268]) Olkoon

$$\omega = \begin{cases} \sqrt{d}, & \text{jos } d \not\equiv 1 \pmod 4, \\ \dfrac{1+\sqrt{d}}{2}, & \text{jos } d \equiv 1 \pmod 4. \end{cases}$$

Lauseen 2.5 ja seurauksen 2.1 nojalla joukon $\mathbb{Q}(\sqrt{d})$ kokonaisluku γ voidaan kirjoittaa muodossa

$$\gamma = (\text{rationaalikokonaisluku}) + (\text{rationaalikokonaisluku})\omega.$$

Koska α, $\beta \in \mathcal{O}$, niin voidaan ne kirjoittaa muodossa

$$\alpha = a + b\omega, \beta = c + e\omega,$$

missä a, b, c, $e \in \mathbb{Z}$. Siis

$$\alpha + \beta = (a + b\omega) + (c + e\omega) = (a + c) + (b + e)\omega$$
$$\alpha - \beta = (a + b\omega) - (c + e\omega) = (a - c) + (b - e)\omega,$$

joten sekä $\alpha + \beta$, $\alpha - \beta \in \mathcal{O}$.

Voidaan kirjoittaa

$$\omega^2 = s\omega + t,$$

missä s, $t \in \mathbb{Z}$. Tarkemmin, jos $d \not\equiv 1 \pmod 4$ (eli $\omega = \sqrt{d}$), niin $s = 0$, $t = d$. Jos

$d \equiv 1 \pmod 4$(eli $\omega = \frac{1+\sqrt{d}}{2}$), niin

$$\begin{aligned}\omega^2 &= \left(\frac{1+\sqrt{d}}{2}\right)^2 \\ &= \frac{1^2 + 2\sqrt{2} + d}{4} \\ &= \frac{1+d}{4} + \frac{1}{2}\sqrt{d} \\ &= \frac{1}{2} + \frac{1}{2}\sqrt{d} - \frac{1}{2} + \frac{1+d}{4} \\ &= \frac{1+\sqrt{d}}{2} + \frac{d-1}{4},\end{aligned}$$

joten $s = 1$, $t = (d-1)/4$, missä luku t on kokonaisluku, koska $d \equiv 1 \pmod 4$. Täten

$$\begin{aligned}\alpha\beta &= (a + b\omega)(c + e\omega) \\ &= ac + (ae + bc)\omega + be\omega^2 \\ &= ac + (ae + bc)\omega + be(s\omega + t) \\ &= (ac + bet) + (bc + bes)\omega,\end{aligned}$$

joka on muotoa $\gamma =$ (rationaalikokonaisluku) + (rationaalikokonaisluku)ω, joten $\alpha\beta \in O$. □

Tiedetään, että luvun normi joukossa $\mathbb{Q}(\sqrt{d})$ on rationaalinen. Tutkitaan seuraavaksi kokonaislukujen normia.

Lause 2.7. *Jos $\alpha \in O$, niin $\mathbf{N}(\alpha) \in \mathbb{Z}$.*

Todistus. (ks. [4, s. 268]) Koska $\alpha \in O$, niin tällöin myös $\overline{\alpha} \in O$. Edellisen lauseen nojalla kahden kokonaisluvun tulo on kokonaisluku, joten $\mathbf{N}(\alpha) = \alpha\overline{\alpha} \in O$. Luku $\mathbf{N}(\alpha) \in \mathbb{Q}$, joten lauseen 2.4 nojalla $\mathbf{N}(\alpha) \in \mathbb{Z}$. □

Edellinen lause voidaan todistaa irrationaaliselle luvulle α myös tarkastelemalla luvun α määrittelevää yhtälöä

$$x^2 + bx + c = 0,$$

missä $b, c \in \mathbb{Z}$. Koska tämän yhtälön ratkaisut ovat α ja $\overline{\alpha}$, niin yhtälön vasen puoli voidaan kirjoittaa muodossa

$$x^2 + bx + c = (x - \alpha)(x - \overline{\alpha}).$$

Kerrotaan yhtälön oikea puoli auki, jolloin saadaan

$$x^2 - \bar{\alpha}x - \alpha x + \alpha\bar{\alpha} = x^2 + (-\alpha - \bar{\alpha})x + \alpha\bar{\alpha}.$$

Nyt

$$\alpha + \bar{\alpha} = -b, \quad \alpha\bar{\alpha} = c.$$

Täten $\alpha + \bar{\alpha}$, $\mathbf{N}(\alpha) = \alpha\bar{\alpha} \in \mathbb{Z}$.

Esimerkki 2.7. Jos $\alpha \in \mathcal{O}$, niin $\alpha^2 + \bar{\alpha}^2 \in \mathbb{Z}$.

Todistus. Oletetaan, että α on kokonaisluku. Lauseen 2.6 perusteella α^2 on kokonaisluku. Täten $\bar{\alpha}^2$ on kokonaisluku. Edelleen, lauseen 2.6 nojalla myös $\alpha^2 + \bar{\alpha}^2$ on kokonaisluku. □

3 Jaollisuus ja alkutekijöihin jakaminen

Määritelmä 3.1. (ks. [4, s. 270]) Olkoot $\alpha, \beta \in O$, ja olkoon $\alpha \neq 0$. Sanotaan, että luku α *jakaa* luvun β, ja kirjoitetaan $\alpha \mid \beta$, jos on olemassa sellainen $\gamma \in O$, että $\beta = \alpha\gamma$. Toisin sanoen $\alpha \mid \beta$, jos $\beta/\alpha \in O$.

Lause 3.1. *Olkoot $\alpha, \beta, \gamma \in O$*

a) Jos $\alpha \mid \beta$ ja $\alpha \mid \gamma$, niin $\overline{\alpha} \mid \overline{\beta}$ ja $\alpha \mid (\beta\delta + \gamma\varepsilon)$ aina, kun $\delta, \varepsilon \in O$.

b) Jos $\alpha \mid \beta$ ja $\beta \mid \gamma$, niin $\alpha \mid \gamma$.

Todistus. (ks. [4, s. 270]) a) Oletetaan, että $\alpha \mid \beta$ ja $\alpha \mid \gamma$. Määritelmän 3.1 nojalla on olemassa sellaiset kokonaisluvut ξ ja η, että $\beta = \alpha\xi$ ja $\gamma = \alpha\eta$. Siis $\overline{\beta} = \overline{\alpha}\overline{\xi}$ ja

$$\beta\delta + \gamma\varepsilon = \alpha\xi\delta + \alpha\eta\varepsilon = \alpha(\xi\delta + \eta\varepsilon).$$

Koska $\xi \in O$, niin $\overline{\xi} \in O$. Koska $\delta, \eta, \varepsilon \in O$, niin lauseen 2.6 nojalla myös $\xi\delta + \eta\varepsilon \in O$. Täten $\overline{\alpha} \mid \overline{\beta}$ ja $\alpha \mid (\beta\delta + \gamma\varepsilon)$.

b) Oletetaan, että $\alpha \mid \beta$ ja $\beta \mid \gamma$. Tällöin on olemassa sellaiset kokonaisluvut, että $\beta = \alpha\xi$ ja $\gamma = \beta\eta$. Siis $\gamma = \alpha\xi\eta$, joten $\alpha \mid \gamma$. □

Huomautus. Olkoot $\alpha, \beta, \gamma, \delta \in O$. Edellisen lauseen nojalla, jos $\alpha \mid \beta$ ja $\alpha \mid \gamma$, niin $\alpha \mid (\beta + \gamma)$, $\alpha \mid (\beta - \gamma)$ ja $\alpha \mid \beta\delta$.

Huomautus. Kun $d < 0$, niin joukossa $\mathbb{Q}(\sqrt{d})$ ei ole mielekästä puhua positiivisista tai negatiivisista luvuista. Jokaisessa positiivisten ja negatiivisten lukujen määritelmässä tulisi esiintyä vähintään seuraavat ominaisuudet:

1) Jokaisen luvun ($\neq 0$) tulee olla joko positiivinen tai negatiivinen, mutta ei molempia.

2) Jos α on positiivinen, niin $-\alpha$ on negatiivinen. Vastaavasti, jos α on negatiivinen, niin $-\alpha$ on positiivinen.

3) Jos α, β ovat positiivisia, niin $\alpha\beta$ on positiivinen.

Esimerkki 3.1. On mahdotonta tehdä sellaista positiivisten ja negatiivisten lukujen määritelmää joukossa $\mathbb{Q}(\sqrt{-1})$, että edellisen huomautuksen kaikki ehdot ovat voimassa.

Todistus. Ehdon 1) nojalla luku $\sqrt{-1}$ on joko positiivinen tai negatiivinen. Oletetaan ensin, että $\sqrt{-1}$ on positiivinen. Ehdon 3) nojalla -1 on positiivinen. Samoin $(-1)^2 = 1$ positiivinen. Tämä on ristiriita kohdan 2) kanssa.

Oletetaan sitten, että $\sqrt{-1}$ on negatiivinen. Tällöin $-\sqrt{-1}$ on positiivinen, joten $-1 = (-\sqrt{-1})^2$ on positiivinen. Ristiriita saadaan vastaavasti kuin edellä. □

Yleisesti, tapauksissa $d < 0$ on mahdotonta tehdä määritelmää positiivisille ja negatiivisille luvuille joukossa $\mathbb{Q}(\sqrt{d})$.

Tarkastellaan seuraavaksi mitä tapahtuu luvuille joukossa $\mathbb{Z} \subset \mathbb{Q}(\sqrt{d})$, kun ne jaetaan tekijöihin, jotka eivät välttämättä ole vain positiivisten lukujen tuloja. Esimerkiksi luku 8 voidaan jakaa tekijöihin usealla eri tavalla:

$$8 = 2 \cdot 2 \cdot 2$$
$$8 = 1 \cdot 2 \cdot 2 \cdot 1 \cdot 1 \cdot 2$$
$$8 = (-2) \cdot (-2) \cdot 2$$
$$8 = (-1) \cdot (-2) \cdot (-1) \cdot (-1) \cdot 2 \cdot (-2) \cdot (-1)$$

Tapauksista nähdään minkä vuoksi lukuja ± 1 ei ole hyödyllistä kutsua alkuluvuiksi. Kutsutaan lukuja 1 ja -1 joukon $\mathbb{Z}$ *yksiköiksi*.

Jos p on rationaalinen alkuluku, niin lukuja p ja $-p$ kutsutaan *liitännäisluvuiksi*. Positiivisten rationaalikokonaislukujen alkutekijähajotelman yksikäsitteisyyslause voidaan korvata hieman yleisemmällä *Rationaalikokonaislukujen alkutekijähajotelman yksikäsitteisyyslauseella*.

Lause 3.2. *Jos $n \in \mathbb{Z}$ ja $n \neq 0$, niin kaksi mielivaltaista luvun n alkutekijähajotelmaa ovat samat tekijöiden järjestystä ja alkulukujen merkkiä lukuunottamatta.*

Todistus. (vrt. [4, s. 272]) Olkoon $n \in \mathbb{Z}$ ja $n \neq 0$. Oletetaan

$$n = n_1 \cdot n_2 \cdots n_s = m_1 \cdot m_2 \cdots m_t$$

missä $n_1, n_2, \ldots, n_s, m_1, m_2, \ldots, m_t$ ovat alkulukuja tai niiden vastalukuja.

Nyt on olemassa sellaiset $u_1, u_2, \ldots, u_s, v_1, v_2, \ldots, v_t \in \{1, -1\}$, että $u_1 n_1, \ldots, u_s n_s, v_1 m_1, \ldots, v_t m_t \in \mathbb{Z}_+$

Alkutekijäharjotelman yksikäsitteisyyslauseen nojalla joukot $\{u_1 n_1, \cdots, u_s n_s\}$ ja $\{v_1 m_1, \cdots, v_t m_t\}$ ovat samoja. Väite seura tästä. □

Vastaavia tilanteita tekijähajotelmissa tulee, kun tarkastellaan joukkoa $\mathbb{Q}(\sqrt{d})$. Nyt, jos ε, $\delta \in \mathbb{Q}(\sqrt{d})$ ja $\varepsilon\delta = 1$, niin tällöin ε ja δ voidaan lisätä tekijähajotelmaan niin useasti kuin halutaan. Esimerkiksi, jos α, β, $\gamma \in \mathcal{O}$ ja $\gamma = \alpha\beta$, niin

$$\gamma = \varepsilon\alpha\delta\beta = (\delta)(\delta)(\delta)(\alpha)(\varepsilon)(\varepsilon)(\varepsilon\beta),$$

ja niin edelleen. Näin tämän esimerkin ε ja δ ovat samassa roolissa joukossa $\mathbb{Q}(\sqrt{d})$, kuin -1 on joukossa $\mathbb{Q}$. Koska $\varepsilon\delta = 1$, ja ε, $\delta \in \mathcal{O}$, niin $\varepsilon \mid 1$.

Määritelmä 3.2. (ks. [4, s. 273]) Kokonaislukua $\varepsilon \in \mathbb{Q}(\sqrt{d})$ kutsutaan *yksiköksi*, jos $\varepsilon \mid 1$. Erityisesti 1 ja -1 ovat aina yksiköitä joukossa $\mathbb{Q}(\sqrt{d})$.

Lause 3.3. *Jos ε_1 ja ε_2 ovat yksiköitä joukossa $\mathbb{Q}(\sqrt{d})$, niin $\overline{\varepsilon_1}$, $\varepsilon_1\varepsilon_2$, $\varepsilon_1/\varepsilon_2$ ovat yksiköitä joukossa $\mathbb{Q}(\sqrt{d})$. Erityisesti $1/\varepsilon_2$ on yksikkö. Edelleen, $\varepsilon \in \mathcal{O}$ on yksikkö, jos ja vain jos $\boldsymbol{N}(\varepsilon) = \pm 1$.*

Todistus. (ks. [4, s. 273]) Oletetaan, että ε_1 ja ε_2 ovat yksiköitä joukossa $\mathbb{Q}(\sqrt{d})$. Tällöin ne ovat kokonaislukuja, ja tällöin on olemassa sellaiset δ_1, $\delta_2 \in \mathcal{O}$, että $\varepsilon_1\delta_1 = \varepsilon_2\delta_2 = 1$. Siis $\overline{\varepsilon_1}$, $\varepsilon_1\varepsilon_2$, $\overline{\delta_1}$, $\delta_2 \in \mathcal{O}$ ja

$$\overline{\varepsilon_1}\,\overline{\delta_1} = \overline{\varepsilon_1\delta_1} = \overline{1} = 1,$$
$$(\varepsilon_1\varepsilon_2)(\delta_1\delta_2) = (\varepsilon_1\delta_1)(\varepsilon_2\delta_2) = 1,$$

joten $\overline{\varepsilon_1}$ ja $\varepsilon_1\varepsilon_2$ ovat yksiköitä. Edelleen

$$\frac{\varepsilon_1}{\varepsilon_2} = \frac{\varepsilon_1\delta_2}{\varepsilon_2\delta_2} = \frac{\varepsilon_1\delta_2}{1} = \varepsilon_1\delta_2$$

on kokonaisluku ja $(\varepsilon_1/\varepsilon_2)(\varepsilon_2\delta_1) = (\varepsilon_1\delta_2)(\varepsilon_2\delta_1) = 1$, missä $\varepsilon_2\delta_1 \in \mathcal{O}$. Siis $\varepsilon_1/\varepsilon_2$ on yksikkö.

Oletetaan seuraavaksi, että $\varepsilon \in \mathcal{O}$ ja $\mathbf{N}(\varepsilon) = \pm 1$. Siis myös $\overline{\varepsilon}$, $-\overline{\varepsilon} \in \mathcal{O}$. Tällöin oltava joko $\mathbf{N}(\varepsilon) = 1$, jolloin

$$\varepsilon\overline{\varepsilon} = \mathbf{N}(\varepsilon) = 1$$

tai $\mathbf{N}(\varepsilon) = -1$, jolloin

$$\varepsilon(-\overline{\varepsilon}) = -\mathbf{N}(\varepsilon) = 1.$$

Molemmissa tapauksissa nähdään, että ε on yksikkö.

Kääntäen, oletetaan, että ε on yksikkö. On siis olemassa sellainen $\delta \in \mathcal{O}$, että $\varepsilon\delta = 1$, joten

$$\mathbf{N}(\varepsilon)\mathbf{N}(\delta) = \mathbf{N}(\varepsilon\delta) = \mathbf{N}(1) = 1.$$

Koska $\mathbf{N}(\varepsilon), \mathbf{N}(\delta) \in \mathbb{Z}$ ja niiden tulo on 1, niin joko $\mathbf{N}(\varepsilon) = \mathbf{N}(\delta) = 1$ tai $\mathbf{N}(\varepsilon) = \mathbf{N}(\delta) = -1$. Siis $\mathbf{N}(\varepsilon) = \pm 1$. □

Huomautus. Lauseessa 3.3 Luvun ε rajoittaminen kokonaisluvuksi on tarpeellista. Esimerkiksi $\mathbf{N}(\frac{3}{5} + \frac{4}{5}\sqrt{-1}) = 1$, mutta koska $\frac{3}{5} + \frac{4}{5}\sqrt{-1}$ ei ole kokonaisluku joukossa $\mathbb{Q}(\sqrt{-1})$, niin se ei ole yksikkö.

Esimerkki 3.2. Jos ε on yksikkö ja $\sqrt{\varepsilon} \in \mathcal{O}$, niin $\sqrt{\varepsilon}$ on yksikkö.

Todistus. Nyt ε on yksikkö, joten $-\varepsilon$ on yksikkö. Koska $\sqrt{\varepsilon} \in \mathcal{O}$ ja

$$\mathbf{N}(\sqrt{\varepsilon}) = (\sqrt{\varepsilon})(-\sqrt{\varepsilon}) = -\varepsilon,$$

niin on oltava $-\varepsilon = \pm 1$. Siis $\sqrt{\varepsilon}$ on yksikkö. □

Esimerkki 3.3. Jos $\varepsilon_1\varepsilon_2$ on yksikkö, missä $\varepsilon_1, \varepsilon_2 \in \mathcal{O}$, niin ε_1 on yksikkö ja ε_2 on yksikkö.

Todistus. Oletetaan, että $\varepsilon_1\varepsilon_2$ on yksikkö. On siis olemassa sellainen $\delta \in \mathcal{O}$, että $\varepsilon_1\varepsilon_2\delta = 1$, joten

$$\mathbf{N}(\varepsilon_1\varepsilon_2)\mathbf{N}(\delta) = \mathbf{N}(\varepsilon_1\varepsilon_2\delta) = \mathbf{N}(1) = 1.$$

Koska $\varepsilon_1, \varepsilon_2, \delta \in \mathcal{O}$, niin lauseen 3.3 nojalla $\mathbf{N}(\varepsilon_1), \mathbf{N}(\varepsilon_2), \mathbf{N}(\delta) \in \mathbb{Z}$. Täten oltava $\mathbf{N}(\varepsilon_1) = \pm 1$ ja $\mathbf{N}(\varepsilon_2) = \pm 1$, joten $\varepsilon_1, \varepsilon_2$ ovat yksiköitä. □

Esimerkki 3.4. Luku $2 + \sqrt{7}$ ei ole yksikkö joukossa $\mathbb{Q}(\sqrt{7})$.

Todistus. Huomataan, että

$$\mathbf{N}(2 + \sqrt{7}) = (2 + \sqrt{7})(2 - \sqrt{7}) = 4 - 7 = -3 \neq \pm 1,$$

joten $2 + \sqrt{7}$ ei ole yksikkö joukossa $\mathbb{Q}(\sqrt{7})$. □

Esimerkki 3.5. Luku $\frac{7+\sqrt{53}}{2}$ on yksikkö joukossa $\mathbb{Q}(\sqrt{53})$.

Todistus. Huomataan, että

$$\begin{aligned}\mathbf{N}\left(\frac{7+\sqrt{53}}{2}\right) &= \left(\frac{7+\sqrt{53}}{2}\right)\left(\frac{7-\sqrt{53}}{2}\right)\\ &= \frac{49-53}{4}\\ &= -1.\end{aligned}$$

Lauseen 2.5 kohdan b) nojalla $\frac{7+\sqrt{53}}{2}$ on kokonaisluku, joten $\frac{7+\sqrt{53}}{2}$ on yksikkö joukossa $\mathbb{Q}(\sqrt{53})$. □

Tarkastellaan seuraavaksi kompleksisten neliökuntien yksiköitä ja reaalineliökuntien yksiköiden lukumäärää.

Apulause 3.1. *Fermat- Pellin yhtälöllä*

$$x^2 - dy^2 = 1,$$

missä $0 < d \in \mathbb{Q}$ ja $\sqrt{d}$ on irrationaalinen, on äärettömän monta rationaalikokonaislukuratkaisua.

Todistus. (ks. [6, s. 66]) Sivuutetaan. □

Lause 3.4. *a) Jos $d < 0$, $d \neq -1$, $d \neq -3$, niin joukossa $\mathbb{Q}(\sqrt{d})$ on täsmälleen kaksi yksikköä: ± 1.*

b) Joukossa $\mathbb{Q}(\sqrt{-1})$ on täsmälleen neljä yksikköä: ± 1 ja $\pm\sqrt{-1}$.

c) Joukossa $\mathbb{Q}(\sqrt{-3})$ on täsmälleen kuusi yksikköä: ± 1, $\pm(-1+\sqrt{-3})/2$ ja $\pm(-1-\sqrt{-3})/2$.

d) Jos $d > 0$, niin joukossa $\mathbb{Q}(\sqrt{d})$ on äärettömän monta yksikköä.

Todistus. (vrt. [4, s. 274]) Jaetaan todistus osiin seuraavasti:

1) $d < 0$ ja $d \not\equiv 1 \pmod 4$

2) $d < 0$ ja $d \equiv 1 \pmod 4$

3) $d > 0$

1) Oletetaan, että $d < 0$ ja $d \not\equiv 1 \pmod 4$. Nyt joukon $\mathbb{Q}(\sqrt{d})$ kokonaisluvut ovat muotoa $\alpha = a + b\sqrt{d}$, missä $a, b \in \mathbb{Z}$. Jos α on yksikkö, niin $\mathbf{N}(\alpha) = \pm 1$. Lauseen 2.4 nojalla normit eivät ole negatiivisia, kun $d < 0$, joten $\mathbf{N}(\alpha) = 1$. Tiedetään, että

$$\mathbf{N}(\alpha) = a^2 - b^2 d = a^2 + b^2(-d).$$

Tarkastellaan ensiksi tapausta $d \neq -1$. Tällöin siis $d \in \{-2, -4, -5, -6, -8, \ldots\}$. Nyt $d \leq -2$ (ja siten $-d \geq 2$), joten $\mathbf{N}(\alpha) \geq a^2 + 2b^2$. Jos $b \neq 0$, jolloin $b^2 \geq 1$, niin

$$\mathbf{N}(\alpha) \geq a^2 + 2 \cdot 1 \geq 2,$$

joten α ei ole yksikkö. Siis, jos α on yksikkö ja $d \leq -2$, niin on oltava $b = 0$, jolloin $\mathbf{N}(\alpha) = a^2 = 1$. Täten $a = \pm 1$, joten $\alpha = \pm 1 + 0\sqrt{d} = \pm 1$. Siis, kun $d \leq -2$, $d \not\equiv 1 \pmod 4$, niin ainoat yksiköt joukossa $\mathbb{Q}(\sqrt{d})$ ovat ± 1.

Oletetaan sitten, että $d = -1$ ja $a,b \in \mathbb{Z}$. Nyt $1 = \mathbf{N}(\alpha) = a^2 - b^2 d = a^2 + b^2$, olettaen, että α on yksikkö. Nähdään, että $a^2 + b^2 \leq 1$, ainoastaan jos $|a| \leq 1$ ja $|b| \leq 1$. Tässä $a^2 + b^2 = 1$ vain, jos $a = \pm 1$ ja $b = 0$, tai $a = 0$ ja $b = \pm 1$. Tästä saadaan, että joukon $\mathbb{Q}(\sqrt{-1})$ ainoat mahdolliset yksiköt ovat ± 1 ja $\pm\sqrt{-1}$.

2) Oletetaan seuraavaksi, että $d < 0$ ja $d \equiv 1 \pmod 4$. Tässä tapauksen joukon $\mathbb{Q}(\sqrt{d})$ kokonaisluvut ovat muotoa

$$\alpha = \frac{a + b\sqrt{d}}{2},$$

missä $a, b \in \mathbb{Z}$ ovat molemmat joko parillisia tai parittomia. Tällöin

$$\begin{aligned}
\mathbf{N}(\alpha) &= \alpha\overline{\alpha} \\
&= \frac{a + b\sqrt{d}}{2}\frac{a - b\sqrt{d}}{2} \\
&= \frac{a^2 - b^2\sqrt{d}\sqrt{d}}{4} \\
&= \frac{a^2 + b^2(-d)}{4}.
\end{aligned}$$

Koska $d < 0$, niin α on yksikkö, jos ja vain jos $\mathbf{N}(\alpha) = 1$. Siis

$$\begin{aligned}
\frac{a^2 + b^2(-d)}{4} &= 1 \\
a^2 + b^2(-d) &= 4
\end{aligned}$$

Tarkastellaan tapausta $d \neq -3$. Tällöin siis $d \in \{-7, -11, \ldots\}$. Nyt, jos $b \neq 0$, niin

$$a^2 + b^2(-d) \geq a^2 + 7b^2 \geq a^2 + 7 \cdot 1 \geq 7 > 4,$$

ja siten, kun α on yksikkö, niin on oltava $b = 0$. Tässä tapauksessa $4 = \mathbf{N}(a) = a^2$, joten $a = \pm 2$ ja $\alpha = \pm 1$. Siis, jos $d \leq -7$ ja $d \equiv 1 \pmod 4$, niin ainoat mahdolliset yksiköt joukossa $\mathbb{Q}(\sqrt{d})$ ovat ± 1.

Oletetaan sitten, että $d = -3$. Jos α on yksikkö, niin saadaan

$$a^2 + 3b^2 = 4.$$

Jos $|b| \geq 2$, niin $a^2 + 3b^2 \geq 12$, ja siten jos $a^2 + 3b^2 = 4$, niin ainoat mahdollisuudet luvulle b ovat $b = \pm 1$ tai $b = 0$.

- Oletetaan, että $b = 0$. Tällöin $a = \pm 2$, joten $\alpha = \pm 1$.
- Oletetaan, että $b = 1$. Tällöin $a = \pm 1$, joten $\alpha = \pm 1 + \sqrt{-3}$.
- Oletetaan, että $b = -1$. Tällöin $a = \pm 1$, joten $\alpha = \pm 1 - \sqrt{-3}$.

Siis ainoat mahdolliset yksiköt joukossa $\mathbb{Q}(\sqrt{-3})$ ovat ± 1, $(\pm 1 \pm \sqrt{-3})/2$.

3) Oletetaan, että $d > 0$. Näytetään, että on olemassa äärettömän monta yksikköä, jotka ovat muotoa

$$\alpha = a + b\sqrt{d}.$$

Osoitetaan, että yksiköitä $\alpha = a + b\sqrt{d}$, missä $a, b \in \mathbb{Z}$, joilla $\mathbf{N}(\alpha) = 1$, on äärettömän monta. Oletetaan, että $\mathbf{N}(\alpha) = 1$. Tällöin

$$a^2 - db^2 = 1.$$

Koska $\sqrt{d}$ on irrationaalinen, niin apulauseen 3.1 perusteella on olemassa äärettömän monta kokonaislukuratkaisua a ja b tälle yhtälölle. Siis joukossa $\mathbb{Q}(\sqrt{d})$ on äärettömän monta yksikköä. □

Huomautus. Olkoon $\alpha \in \mathcal{O}$. Jos $\mathbf{N}(\alpha) = 0$, niin $\alpha = 0$, ja jos $|\mathbf{N}(\alpha)| = 1$, niin α on yksikkö. Siis $0 \neq \alpha \in \mathcal{O}$ on kokonaisluku ja α ei ole yksikkö, jos ja vain jos $|\mathbf{N}(\alpha)| \geq 2$.

Määritelmä 3.3. (ks. [4, s. 276]) Olkoon $\pi \in O$, $\pi \neq 0$ ja π ei ole yksikkö. Lukua π kutsutaan *alkuluvuksi* joukossa $\mathbb{Q}(\sqrt{d})$, jos jokaisessa luvun π kokonaislukuhajotelmassa $\pi = \alpha\beta$, joko α on yksikkö tai β on yksikkö. Kutsutaan jatkossa joukon $\mathbb{Z}$ alkulukuja *rationaalialkuluvuiksi*. Lukua, joka ei ole nolla, yksikkö eikä alkuluku kutsutaan *yhdistetyksi luvuksi* joukossa $\mathbb{Q}(\sqrt{d})$. Toisin sanoen yhdistetty luku on sellainen kahden luvun tulo joukossa $\mathbb{Q}(\sqrt{d})$, että kumpikaan tulon tekijöistä ei ole nolla eikä yksikkö.

Esimerkki 3.6. Rationaalialkuluku 2 ei ole alkuluku joukossa $\mathbb{Q}(\sqrt{3})$. Nimittäin

$$2 = (1 + \sqrt{3})(-1 + \sqrt{3}),$$

ja

$$\mathbf{N}(1 + \sqrt{3}) = (1 + \sqrt{3})(1 - \sqrt{3}) = -2 = (-1 + \sqrt{3})(-1 - \sqrt{3}) = \mathbf{N}(-1 + \sqrt{3}),$$

missä kumpikaan luvuista $1 + \sqrt{3}$, $-1 + \sqrt{3}$ ei ole yksikkö.

Lause 3.5. *Jos $\alpha \in O$ ja $\boldsymbol{N}(\alpha)$ on rationaalialkuluku, niin α on alkuluku.*

Todistus. (ks. [4, s. 277]) Koska $\mathbf{N}(\alpha)$ on rationaalialkuluku, niin lauseiden 2.4 ja 3.3 nojalla $\alpha \neq 0$ ja α ei ole yksikkö. Oletetaan, että $\alpha = \beta\gamma$, missä $\beta, \gamma \in O$. Nyt

$$\mathbf{N}(\alpha) = \mathbf{N}(\beta\gamma) = \mathbf{N}(\beta)\mathbf{N}(\gamma),$$

missä $\mathbf{N}(\beta), \mathbf{N}(\gamma) \in \mathbb{Z}$. Koska $\mathbf{N}(\alpha)$ on rationaalialkuluku, niin joko $\mathbf{N}(\beta) = \pm 1$ tai $\mathbf{N}(\gamma) \pm 1$. Siis toinen luvuista β, γ on yksikkö, joten α on alkuluku. □

Esimerkki 3.7. Luku $3 + 2\sqrt{-5}$ on alkuluku joukossa $\mathbb{Q}(\sqrt{-5})$.

Todistus. Luku $3 + 2\sqrt{-5} \in O_{\mathbb{Q}(\sqrt{-5})}$ lauseen 2.5 kohdan a) nojalla. Nyt

$$\mathbf{N}(3 + 2\sqrt{-5}) = (3 + 2\sqrt{-5})(3 - 2\sqrt{-5}) = -11,$$

joka on rationaalialkuluku, joten lauseen 3.5 perusteella $3 + 2\sqrt{-5}$ on alkuluku joukossa $\mathbb{Q}(\sqrt{-5})$. □

Esimerkki 3.8. Luku 3 on kahden alkuluvun tulo joukossa $\mathbb{Q}(\sqrt{6})$.

Todistus. Luku 3 voidaan kirjoittaa muodossa:

$$3 = (3 + \sqrt{6})(3 - \sqrt{6}),$$

missä luvut $3 + \sqrt{6}$, $3 - \sqrt{6}$ ovat alkulukuja, koska ne ovat kokonaislukuja lauseen 2.5 kohdan a) nojalla ja

$$\mathbf{N}(3 + \sqrt{6}) = \mathbf{N}(3 - \sqrt{6}) = 3,$$

joka on rationaalialkuluku. Siis lauseen 3.5 nojalla luku 3 voidaan kirjoittaa kahden alkuluvun tulona joukossa $\mathbb{Q}(\sqrt{6})$. □

Määritelmä 3.4. (ks. [4, s. 278]) Oletetaan, että $0 \neq \alpha, \beta \in O$. Jos $\alpha = \beta\varepsilon$, missä ε on yksikkö, niin luvun α sanotaan olevan luvun β *liitännäisluku*. Toisin sanoen α on luvun β liitännäisluku, jos ja vain jos α/β on yksikkö. Jos α ja β ovat toistensa liitännäislukuja, niin sanotaan, että α ja β ovat *liitännäisiä*.

Tämän määritelmän nojalla, jokainen kokonaisluku on itsensä liitännäisluku.

Huomautus. Termi liitännäisluku esiintyy esimerkiksi lähteessä [6].

Lause 3.6. *Olkoot* $0 \neq \alpha, \beta \in O$.

a) Luku α on luvun β liitännäisluku, jos ja vain jos luku β on luvun α liitännäisluku.

b) Luvut α ja β ovat liitännäisiä, jos ja vain jos $\alpha \mid \beta$ ja $\beta \mid \alpha$.

c) Jos α ja β ovat liitännäisiä, niin

$$\gamma \mid \alpha \;\Rightarrow\; \gamma \mid \beta \quad ja \quad \alpha \mid \delta \;\Rightarrow\; \beta \mid \delta.$$

d) Jos α on alkuluku, niin jokainen luvun α liitännäisluku on alkuluku. Vastaavasti, jos α on yhdistetty luku, niin jokainen luvun α liitännäisluku on yhdistetty luku.

Todistus. (vrt. [4, s. 278]) a) Oletetaan, että α on luvun β liitännäisluku, eli on olemassa sellainen yksikkö ε, että $\alpha = \beta\varepsilon$. Koska ε on yksikkö, niin $(1/\varepsilon)$ on myös yksikkö. Siis $\beta = \alpha(1/\varepsilon)$, joten β on luvun α liitännäisluku. Vastaavasti voidaan todistaa väitteen toinen suunta.

b) Jos kokonaisluvut α ja β ovat toistensa liitännäislukuja, niin on olemassa sellainen yksikkö ε, että $\alpha = \beta\varepsilon$ ja $\beta = \alpha(1/\varepsilon)$. Koska ε ja $1/\varepsilon$ ovat yksiköitä ja siten myös kokonaislukuja, niin $\beta \mid \alpha$ ja $\alpha \mid \beta$.

Oletetaan, että $\beta \mid \alpha$ ja $\alpha \mid \beta$. Tällöin $\beta = \alpha\varepsilon$ ja $\alpha = \beta\gamma$, missä $\varepsilon, \gamma \in \mathcal{O}$. Nyt

$$\varepsilon\gamma = (\beta/\alpha)(\alpha/\beta) = (\alpha\beta/\alpha\beta) = 1,$$

joten ε ja γ ovat yksiköitä. Siis α, β ovat liitännäisiä.

c) Olkoot α, β liitännäisiä. Oletetaan, että $\gamma \mid \alpha$ ja $\alpha \mid \delta$. Koska $\gamma \mid \alpha$ ja kohdan b) nojalla $\alpha \mid \beta$, niin lauseen 3.1 perusteella $\gamma \mid \beta$. Koska $\beta \mid \alpha$ ja $\alpha \mid \delta$, niin lauseen 3.1 perusteella $\beta \mid \delta$.

d) Lauseen 3.3 nojalla kaikkien yksiköiden liitännäisluvut ovat yksiköitä ja siten ei-yksiköiden liitännäisluvut ovat ei-yksiköitä. Oletetaan, että α, $\beta \neq 0$ ovat liitännäisiä ei-yksiköitä joukossa $\mathbb{Q}(\sqrt{d})$. Siis α, β on joko alkuluku tai yhdistetty luku. Näytetään seuraavaksi, että α, β ovat joko molemmat alkulukuja tai molemmat yhdistettyjä lukuja.

Oletetaan, että α on alkuluku ja β on yhdistetty luku (käänteinen tapaus vastaavasti). Nyt voidaan kirjoittaa $\beta = \gamma\delta$, missä γ, δ eivät ole yksiköitä. Koska α, β ovat liitännäisiä, niin on olemassa sellainen yksikkö ε, että $\alpha = \varepsilon\beta = \varepsilon(\gamma\delta) = \gamma(\delta\varepsilon)$. Koska γ ei ole yksikkö ja $(\delta\varepsilon)$ on ei-yksikön liitännäisluku, niin $(\delta\varepsilon)$ ei ole yksikkö. Nyt α on jaettu kahteen tekijään, joista kumpikaan ei ole yksikkö. Tämä on risiriidassa oletuksen α on alkuluku kanssa. Siis α, β ovat joko molemmat alkulukuja tai molemmat yhdistettyjä lukuja. □

Esimerkki 3.9. Jos π_1, π_2 ovat alkulukuja joukossa $\mathbb{Q}(\sqrt{d})$ ja $\pi_1 \mid \pi_2$, niin π_1, π_2 ovat liitännäisiä.

Todistus. Koska $\pi_1 \mid \pi_2$, niin voidaan kirjoittaa

$$\pi_2 = \varepsilon\pi_1,$$

missä $\varepsilon \in \mathcal{O}$. Koska π_1, π_2 ovat alkulukuja, niin ε on yksikkö. Nyt

$$\pi_1 = \frac{1}{\varepsilon}\pi_2,$$

joten $\pi_2 \mid \pi_1$. Täten lauseen 3.6 nojalla π_1 ja π_2 ovat liitännäisiä. □

Lause 3.7. *Oletetaan, että* $0 \neq \alpha_1, \alpha_2, \ldots, \alpha_n \in O$ *ja*

$$\alpha = \alpha_1 \alpha_2 \cdots \alpha_n,$$

missä $n > \log_2(|\boldsymbol{N}(\alpha)|)$. *Tällöin vähintään yksi luvuista* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *on yksikkö. Tästä seuraa, että mikäli* α *ei ole yksikkö, niin se voidaan esittää äärellisen monen alkuluvun tulona joukossa* $\mathbb{Q}(\sqrt{d})$.

Todistus. (vrt. [4, s. 279]) Oletetaan, ettei mikään luvuista α_j ole yksikkö. Siis jokaiselle indeksille j, missä $1 \leq j \leq n$, pätee $|\mathbf{N}(\alpha_j)| \geq 2$. Nyt

$$\begin{aligned} |\mathbf{N}(\alpha)| &= |\mathbf{N}(\alpha_1)\mathbf{N}(\alpha_2)\cdots\mathbf{N}(\alpha_n)| \\ &= |\mathbf{N}(\alpha_1)| \cdot |\mathbf{N}(\alpha_2)| \cdots |\mathbf{N}(\alpha_n)| \\ &\geq 2 \cdot 2 \cdots 2 \\ &= 2^n. \end{aligned}$$

Siis $|\mathbf{N}(\alpha)| \geq 2^n$, eli $\log_2(|\mathbf{N}(\alpha)|) \geq \log_2(2^n) = n$. Tämä on ristiriidassa oletuksen $n > \log_2(|\mathbf{N}(\alpha)|)$ kanssa, joten vähintään yksi luvuista $\alpha_1, \alpha_2, \ldots, \alpha_n$ on yksikkö.

Oletetaan seuraavaksi, että kokonaisluku $\alpha \neq 0$ ei ole yksikkö joukossa $\mathbb{Q}(\sqrt{d})$. Osoitetaan, että α voidaan kirjoittaa yhden tai useamman alkuluvun tulona. Jos α on alkuluku, niin asia on triviaalisti selvä.

Oletetaan, että α on yhdistetty luku, jolloin voidaan kirjoittaa $\alpha = \alpha_1\beta_1$, missä kumpikaan kokonaisluvuista α_1, β_1 ei ole yksikkö. Mikäli luvut ovat alkulukuja, niin väite todistettu. Oletetaan, etteivät molemmat luvuista α_1, β_1 ole alkulukuja. Tällöin voidaan olettaa, että β_1 on yhdistetty luku. Merkitään $\beta_1 = \alpha_2\beta_2$, missä luvut α_2, β_2 eivät ole yksiköitä. Siis $\alpha = \alpha_1\alpha_2\beta_2$ on kolmen luvun tulo, missä mikään luvuista α_1, α_2, β_2 ei ole yksikkö. Jälleen, mikäli jokin luvuista α_1, α_2, β_2 on alkuluku, niin väite todistettu todeksi. Jatkamalla todistusta vastaavasti saadaan

$$\alpha = \alpha_1\alpha_2 \cdots \alpha_{n-1}\beta_{n-1},$$

missä mikään yhtälön oikean puolen luvuista ei ole yksikkö. Jollakin $n \leq \log_2 |\mathbf{N}(\alpha)|$ saadaan alkuluvut $\alpha_1,\ldots,\alpha_{n-1},\beta_{n-1}$. Mikäli ei, niin toistetaan menetelmää kunnes saavutetaan $n > \log_2 |\mathbf{N}(\alpha)|$. Tällöin yhtälön oikealla puolella on n tekijää ja lauseen alkuosan nojalla vähintään yksi näistä on yksikkö. Näin saadaan luvulle α äärellinen alkutekijähajotelma. □

4 Yksikäsitteinen tekijähajotelma ja Euklideen alue

Määritelmä 4.1. (vrt. [5, s. 82] ja [4, s. 281]) Oletetaan, että joukossa $\mathbb{Q}(\sqrt{d})$ on seuraava ominaisuus voimassa: Jos ei-yksiköllä $0 \neq \alpha \in O$ on tekijähajotelmat

$$\alpha = \varepsilon\pi_1\pi_2\cdots\pi_r, \quad \alpha = \varepsilon'\pi_1'\pi_2'\cdots\pi_s',$$

missä ε, ε' ovat yksiköitä ja π_1, π_2, …, π_r, π_1', …, π_s' ovat alkulukuja, niin $r = s$ ja on olemassa sellainen bijektio $\sigma : \{1,\ldots,r\} \to \{1,\ldots,s\}$, että $\pi_{\sigma(i)}$ ja π_i ovat liitännäisiä kaikilla $i \in \{1,\ldots,r\}$. Tällöin kokonaislukujen joukko O on *faktoriaalinen rengas*.

Esimerkki 4.1. Joukko $O_{\mathbb{Q}(\sqrt{-5})}$ ei ole faktoriaalinen rengas.

Todistus. Huomataan aluksi, että jos $a + b\sqrt{-5} \in O$, niin sen normi

$$\mathbf{N}(a + b\sqrt{-5}) = a^2 + 5b^2.$$

Erityisesti, jos $a, b \in \mathbb{Z}$, niin normin pienimmät mahdolliset arvot ovat $0, 1, 4, 5, 6, 9$. Täten, jos $\mathbf{N}(\alpha) \in \{4, 5, 6, 9\}$, niin α on alkuluku.

Tarkastellaan lukua $6 \in \mathbb{Q}(\sqrt{d})$, jolla on kaksi tekijähajotelmaa

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Nyt

$$\begin{aligned} \mathbf{N}(2) &= 4 \\ \mathbf{N}(3) &= 9 \\ \mathbf{N}(1 + \sqrt{-5}) = \mathbf{N}(1 - \sqrt{-5}) &= 6. \end{aligned}$$

Siis 2, 3, $1 + \sqrt{-5}$ ja $1 - \sqrt{-5}$ ovat alkulukuja joukossa $\mathbb{Q}(\sqrt{-5})$. Kuitenkaan luku 2 ei ole liitännäinen lukujen $1 \pm \sqrt{-5}$ kanssa. Täten $O_{\mathbb{Q}(\sqrt{-5})}$ ei ole faktoriaalinen rengas. □

Apulause 4.1. Olkoon $\alpha \in O$ ja π alkuluku. Jos $\pi \mid \alpha$, niin α ei ole yksikkö.

Todistus. Tehdään vastaoletus, että α on yksikkö. Nyt $\pi \mid \alpha$, eli $\alpha = \pi\gamma$ jollain $\gamma \in \mathcal{O}$. Siispä $1 = \pi\gamma\alpha^{-1}$, joten $\pi \mid 1$, eli π on yksikkö, mikä on ristiriita. □

Lause 4.1. *Kokonaislukujen joukko $\mathcal{O}$ on faktoriaalinen rengas, jos ja vain jos joukossa $\mathbb{Q}(\sqrt{d})$ pätee*

$$\pi \mid \alpha\beta \Rightarrow \pi \mid \alpha \text{ tai } \pi \mid \beta$$

aina, kun π on alkuluku ja α, $\beta \in \mathcal{O}$.

Todistus. (vrt. [4, s. 282]) Oletetaan aluksi, että kokonaislukujen joukko $\mathcal{O}$ on faktoriaalinen rengas ja $\pi \mid \alpha\beta$, missä π on alkuluku ja α, $\beta \in \mathcal{O}$. Koska $\pi \mid \alpha\beta$, niin on olemassa sellainen $\gamma \in \mathcal{O}$, että $\alpha\beta = \pi\gamma$. Lauseen 3.7 nojalla on olemassa sellaiset alkuluvut $\pi_1, \pi_2, \ldots, \pi_n$ ja yksikkö ε joukossa $\mathbb{Q}(\sqrt{d})$, että

$$\gamma = \varepsilon\pi_1\pi_2 \cdots \pi_n.$$

Nyt

$$\alpha\beta = \varepsilon\pi\pi_1\pi_2 \cdots \pi_n$$

on luvun $\alpha\beta$ alkutekijähajotelma. Vastaavasti on olemassa sellaiset alkuluvut

$$\pi_1', \ldots, \pi_r', \pi_1'', \ldots, \pi_s''$$

ja yksiköt ε_1, ε_2, että

$$\alpha = \varepsilon_1\pi_1' \cdots \pi_r', \quad \beta = \varepsilon_2\pi_1'' \cdots \pi_s'',$$

joten

$$\alpha\beta = (\varepsilon_1\varepsilon_2)\pi_1' \cdots \pi_r'\pi_1'' \cdots \pi_s''.$$

Luku $\alpha\beta$ ei ole yksikkö apulauseen 4.1 perusteella, mutta on kuitenkin mahdollista, että jokin luvuista α, β tai γ on yksikkö (mutta sekä α että β eivät voi olla yksiköitä). Tällaisessa tapauksessa on oltava $r = 0$, $s = 0$ tai $n = 0$.

Nyt on olemassa alkutekijähajotelmat:

$$\alpha\beta = \varepsilon\pi\pi_1 \cdots \pi_n = (\varepsilon_1\varepsilon_2)\pi_1' \cdots \pi_r'\pi_1'' \cdots \pi_s''.$$

Yksi oikean puolen yhtälön alkuluvuista on luvun π liitännäisluku, ja näin ollen myös jaollinen luvulla π. Jos $\pi \mid \pi_i'$, jollain $i \in \{1, \ldots r\}$, niin $\pi \mid \alpha$. Jos $\pi \mid \pi_j''$, jollain $i \in \{1, \ldots s\}$, niin $\pi \mid \beta$. Siis π jakaa joko luvun α tai β, tai mahdollisesti molemmat.

Kääntäen, oletetaan, että joukossa $\mathbb{Q}(\sqrt{d})$ pätee

$$\pi \mid \alpha\beta \Rightarrow \pi \mid \alpha \text{ tai } \pi \mid \beta$$

aina, kun π on alkuluku ja $\alpha, \beta \in O$. Oletetaan, että $0 \neq \alpha$ ei ole yksikkö joukossa O ja

$$\alpha = \varepsilon\pi_1\pi_2 \cdots \pi_r = \varepsilon'\pi_1'\pi_2' \cdots \pi_s', \tag{4.1}$$

missä ε, ε' ovat yksiköitä ja π_1, π_2, …, π_r, π_1', π_2', …, π_s' ovat alkulukuja. Voidaan olettaa, että $r \leq s$. Näytetään, että yksi luvuista π_s' on luvun π_1 liitännäisluku. Nyt $\pi_1 \mid \alpha$, joten

$$\pi_1 \mid (\pi_1' \cdots \pi_{s-1}')\pi_s'.$$

Oletuksen nojalla $\pi_1 \mid (\pi_1' \cdots \pi_{s-1}')$ tai $\pi_1 \mid \pi_s'$. Jos $\pi_1 \mid \pi_s'$, niin $\pi_s' = \pi_1\delta$, missä luvun δ on oltava yksikkö, sillä π_s' on alkuluku. Näin ollen π_1, π_s' ovat liitännäisiä. Oletetaan sitten, että $\pi_1 \mid (\pi_1' \cdots \pi_{s-2}')\pi_{s-1}'$. Mikäli π_1, π_{s-1}' eivät ole liitännäisiä, niin jatketaan menetelmää, kunnes löydetään luvun π_1 liitännäisluku alkuluvuista π_2', π_3',…, π_s', tai $\pi_1 \mid \pi_1'$. Jälkimmäisen ollessa voimassa päädytään tapaukseen, jolloin π_1 ja π_1' ovat liitännäisiä.

Ollaan osoitettu, että yksi luvuista $\pi_i'(i \in \{1, \ldots, s\}$ on luvun π_1 liitännäisluku. Uudelleennumeroimalla voidaan olettaa, että π_1' ja π_1 ovat liitännäisiä. Siis $\pi_1' = \varepsilon_1\pi_1$, missä ε_1 on yksikkö. Sijoitetaan tulos yhtälöön (4.1):

$$\varepsilon\pi_2 \cdots \pi_r = (\varepsilon'\varepsilon_1)\pi_2' \cdots \pi_s', \tag{4.2}$$

missä $\varepsilon'\varepsilon_1$ on myös yksikkö.

Toistetaan menetelmä luvulle π_2 luvun π_1 sijaan, jolloin huomataan, että yksi alkuluvuista π_2',…,π_s' on luvun π_2 liitännäisluku. Uudelleennumeroimalla voidaan olettaa, että kyseinen liitännäisluku on π_2'. Siis $\pi_2' = \varepsilon_2\pi_2$, missä ε_2 on yksikkö. Sijoitetaan tulos yhtälöön (4.2):

$$\varepsilon\pi_3 \cdots \pi_r = (\varepsilon'\varepsilon_1\varepsilon_2)\pi_3' \cdots \pi_s',$$

missä $\varepsilon'\varepsilon_1\varepsilon_2$ on yksikkö.

Toistetaan tätä siihen asti, että π'_j on luvun π_j liitännäisluku, kaikilla $1 \leq j \leq r-1$ ja

$$\varepsilon\pi_r = (\varepsilon'\varepsilon_1\varepsilon_2\cdots\varepsilon_{r-1})\pi'_r\cdots\pi'_s, \tag{4.3}$$

missä $\varepsilon'\varepsilon_1\varepsilon_2\cdots\varepsilon_{r-1}$ on yksikkö. Yhtälön (4.3) vasemmalla puolella on alkuluku, joten näin on oltava myös oikealla puolella. Yhtälön oikealla puolella on yhdistetty luku, mikäli $s > r$, ja siksi oltava $s = r$. Nyt $\varepsilon\pi_r = \varepsilon''\pi'_r$, joten $\pi'_r = \varepsilon/\varepsilon''\pi_r$, missä $\varepsilon/\varepsilon''$ on yksikkö. Siis π'_r on luvun π_r liitännäisluku. Täten joukko O on faktoriaalinen rengas. □

Lause 4.2. *Oletetaan, että O on faktoriaalinen rengas. Olkoot α, β ja γ sellaisia kokonaislukuja ja olkoon ε sellainen yksikkö joukossa $\mathbb{Q}(\sqrt{d})$, että luvuilla α, β ei ole muita yhteisiä kokonaislukutekijöitä kuin yksiköt ja $\alpha\beta = \varepsilon\gamma^n$, missä $n \in \mathbb{Z}_+$. Tällöin on olemassa sellaiset yksiköt ε', ε'' ja kokonaisluvut δ, $\zeta \in \mathbb{Q}(\sqrt{d})$, että $\alpha = \varepsilon'\delta^n$ ja $\beta = \varepsilon''\zeta^n$.*

Todistus. (vrt. [4, s. 284]) Oletetaan, että γ on yksikkö. Tällöin $\alpha\beta$ on yksikkö, eli α, β ovat yksiköitä. Tässä tapauksessa väite triviaalisti tosi: valitaan $\varepsilon' = \alpha$, $\varepsilon'' = \beta$, $\delta = \zeta = 1$.

Oletetaan, että $\gamma = 0$. Tällöin $\alpha = 0$ tai $\beta = 0$. Voidaan olettaa, että $\alpha = 0$. Koska $\beta \mid 0$ ja $\beta \mid \beta$, niin β on yksikkö, koska lukujen $\alpha = 0$ ja β yhteiset tekijät ovat yksiköitä. Siis väite on tässäkin tapauksessa tosi, kun valitaan $\delta = 0$, $\zeta = 1$ ja $\varepsilon'' = \beta$.

Oletetaan seuraavaksi, että $\gamma \neq 0$ ei ole yksikkö. Voidaan merkitä

$$\gamma = \pi_1\pi_2\cdots\pi_r,$$

missä $\pi_1,\ldots,\pi_r$ ovat alkulukuja, joista jotkut voivat olla keskenään liitännäisiä.

Todistetaan väite luvulle α (luvun β todistus vastaavasti). Mikäli α on yksikkö, niin asetetaan $\varepsilon = \alpha$ ja $\gamma = 1$. Oletetaan seuraavaksi, että α ei ole yksikkö. Lisäksi $\alpha \neq 0$, koska $\gamma \neq 0$. Näin ollen α voidaan kirjoittaa alkulukujen tulona muodossa

$$\alpha = \pi'_1\pi'_2\cdots\pi'_s.$$

Sijoittamalla hajotelmat yhtälöön $\alpha\beta = \varepsilon\gamma^n$ saadaan

$$\pi'_1\pi'_2\cdots\pi'_s\beta = \varepsilon\pi_1^n\pi_2^n\cdots\pi_r^n. \tag{4.4}$$

Faktoriaalisuuden perusteella π_1' on jonkin luvun π_j liitännäisluku. Voidaan olettaa, että π_1' ja π_1 ovat liitännäisiä. Nyt, jos jokin luvun π_1 liitännäisluku jakaisi luvun β, niin myös $\pi_1' \mid \beta$, joten π_1' olisi lukujen α, β yhteinen tekijä. Oletuksen mukaan tämä on ristiriita, joten $\pi_1' \nmid \beta$. Luvun π_1 tai sen liitännäisluvun tulee esiintyä n kertaa alkulukujen $\pi_1',\ldots,\pi_s'$ joukossa. Erityisesti siis $s \geq n$. Luvut voidaan uudelleennumeroida siten, että $\pi_1',\ldots,\pi_n'$ ovat luvun π_1 liitännäislukuja. Täten on myös olemassa sellaiset yksiköt $\varepsilon_1,\ldots,\varepsilon_n$, että

$$\pi_1' = \varepsilon_1\pi_1, \quad \pi_2' = \varepsilon_2\pi_1, \ \ldots, \ \pi_n' = \varepsilon_n\pi_1,$$

joten

$$\pi_1'\pi_2'\cdots\pi_n' = (\varepsilon_1\varepsilon_2\cdots\varepsilon_n)\pi_1^n.$$

Jos $s = n$, niin lause on todistettu, koska tällöin yhtälön vasen puoli on α.

Oletetaan, että $s > n$. Jaetaan yhtälö (4.4) puolittain luvulla π_1^n, jolloin saadaan

$$(\varepsilon_1\varepsilon_2\cdots\varepsilon_n)\pi_{n+1}'\pi_{n+2}'\cdots\pi_s'\beta = \varepsilon\pi_2^n\pi_3^n\cdots\pi_r^n. \tag{4.5}$$

Faktoriaalisuuden perusteella yksi luvuista π_j, missä $2 \leq j \leq r$, on luvun π_{n+1}' liitännäisluku. Voidaan olettaa, että tämä luku on π_2. Kuten edellä, nähdään, että luvun π_2 tai sen liitännäisluvun tulee esiintyä n kertaa alkulukujen $\pi_{n+1}',\ldots,\pi_s'$ joukossa. Uudelleennumeroidaan luvut jälleen siten, että $\pi_{n+1}',\ldots,\pi_{2n}'$ ovat luvun π_2 liitännäislukuja. Tästä seuraa, että $s \geq 2n$ ja on olemassa sellaiset yksiköt $\varepsilon_{n+1},\ldots,\varepsilon_{2n}$, että

$$\pi_{n+1}' = \varepsilon_{n+1}\pi_2, \quad \pi_{n+2}' = \varepsilon_{n+2}\pi_2, \ \ldots \ ,\pi_{2n}' = \varepsilon_{2n}\pi_2,$$

joten

$$\pi_{n+1}'\cdots\pi_{2n}' = (\varepsilon_{n+1}\ldots\varepsilon_{2n})\pi_2^n.$$

Jos $s = 2n$, niin $\alpha = (\varepsilon_1\ldots\varepsilon_{2n})(\pi_1\pi_2)^n$, ja väite on todistettu.

Mikäli $s > 2n$, niin toistetaan samaa prosessia. Koska luvun α tekijähajotelmassa alkulukuja on äärellinen määrä, niin jossakin kohtaa prosessi päättyy, ja löydetään sellainen k, että $s = kn$. Tällöin on saatu sellaiset yksiköt $\varepsilon_1,\ldots,\varepsilon_{kn}$, että

$$\alpha = \pi_1'\pi_2'\cdots\pi_{kn}' = (\varepsilon_1\varepsilon_2\ldots\varepsilon_{kn})(\pi_1\pi_2\cdots\pi_k)^n.$$

Tämä on haluttua muotoa, kun valitaan

$$\varepsilon' = \varepsilon_1\varepsilon_2\ldots\varepsilon_{kn} \quad \text{ja} \quad \delta = \pi_1\pi_2\cdots\pi_k.$$

□

Apulause 4.2 (Bezout'n lemma)**.** Olkoot $a, b \in \mathbb{Z}$, missä $a \neq 0$ tai $b \neq 0$. Nyt on olemassa sellaiset $r, s \in \mathbb{Z}$, että

$$ar + bs = \text{syt}(a, b)$$

Todistus. (ks. [4, s.22]) Sivuutetaan. □

Lause 4.3. *Olkoot $a, b \in \mathbb{Z}$, missä $a \neq 0$ tai $b \neq 0$, ja olkoon $syt(a, b) = c$. Jos $\alpha \in \mathcal{O}$ on sellainen kokonaisluku, että $\alpha \mid a$ ja $\alpha \mid b$, niin $\alpha \mid c$.*

Erityisesti, jos a ja b ovat keskenään jaottomia, niin niiden yhteiset tekijät joukossa $\mathbb{Q}(\sqrt{d})$ ovat yksiköitä.

Todistus. (ks. [4, s. 285]) Jos $\text{syt}(a, b) = c$, niin apulauseen 4.2 nojalla on olemassa sellaiset $r, s \in \mathbb{Z}$, että $ar + bs = c$. Lauseen 3.1 nojalla, jos $\alpha \mid a$ ja $\alpha \mid b$, niin $\alpha \mid (ar + bs)$, eli $\alpha \mid c$.

Jos a, b ovat keskenään jaottomia, niin $c = 1$, ja koska $\alpha \mid c$, niin α on yksikkö.

□

Määritelmä 4.2. (ks. [4, s. 290]) Neliökuntaa $\mathbb{Q}(\sqrt{d})$ kutsutaan *Eukleideen kunnaksi*, jos siinä pätee seuraava ominaisuus: Jos $\alpha, \beta \in \mathcal{O}$, missä $\beta \neq 0$, niin on olemassa sellaiset $\gamma, \delta \in \mathcal{O}$, että

$$\alpha = \gamma\beta + \delta \quad \text{ja} \quad |\mathbf{N}(\delta)| < |\mathbf{N}(\beta)|.$$

(Jos $d < 0$, niin itseisarvot voidaan poistaa, koska normit ovat ei-negatiivisia.)

Huomautus. (vrt. [5, s. 90-91]) Mikäli $\mathbb{Q}(\sqrt{d})$ on Eukleideen kunta, niin sanotaan, että $\mathcal{O}$ on *Eukleideen alue*.

Määritelmä 4.3. (vrt. [8]) Olkoot $\alpha, \beta, \delta \in \mathcal{O}$. Mikäli

1) $\delta \mid \alpha$ ja $\delta \mid \beta$

2) $\gamma \mid \alpha, \gamma \mid \beta \Rightarrow \gamma \mid \delta$ aina, kun $\gamma \in \mathcal{O}$.

niin δ on lukujen α ja β *suurin yhteinen tekijä*. Merkitään $\text{syt}(\alpha, \beta) = \delta$.

Huomautus. Lukujen α, β suurin yhteinen tekijä ei yleensä ole yksikäsitteinen, eikä sitä välttämättä ole olemassa.

Lause 4.4. *Olkoon $\mathbb{Q}(\sqrt{d})$ Eukleideen kunta, ja olkoot α, $\beta \in O$, missä $\alpha \neq 0$ tai $\beta \neq 0$. Tällöin $\delta = syt(\alpha, \beta)$ on olemassa ja liitännäisyyttä vaille yksikäsitteinen. Lisäksi on olemassa sellaiset ζ, $\eta \in O$, että $\delta = \alpha\zeta + \beta\eta$.*

Todistus. (vrt. [4, s. 291]) *Olemassaolo*: Koska $\alpha \neq 0$ tai $\beta \neq 0$, niin voidaan olettaa, että $\beta \neq 0$. Määritelmän 4.2 mukaan on olemassa sellaiset γ_1, $\beta_1 \in O$, että

$$\alpha = \gamma_1\beta + \beta_1 \quad \text{ja} \quad |\mathbf{N}(\beta)| < |\mathbf{N}(\beta_1)|.$$

Oletetaan ensin, että $\beta_1 = 0$. Tällöin $\beta \mid \alpha$. Koska tietenkin $\beta \mid \beta$ ja

$$\gamma \mid \alpha, \gamma \mid \beta \Rightarrow \gamma \mid \beta,$$

niin $\text{syt}(\alpha, \beta) = \beta$. Oletetaan, että $\beta_1 \neq 0$. Nyt on olemassa sellaiset γ_2, $\beta_2 \in O$, että

$$\beta = \gamma_2\beta_1 + \beta_2 \quad \text{ja} \quad |\mathbf{N}(\beta_1)| < |\mathbf{N}(\beta_2)|.$$

Oletetaan sitten, että $\beta_2 = 0$. Tällöin $\beta_1 \mid \beta$. Nyt $\alpha = \beta_1(\gamma_1\gamma_2 + 1)$, joten $\beta_1 \mid \alpha$. Koska $\beta_1 = \alpha - \gamma_1\beta$, niin $\gamma \mid \alpha, \gamma \mid \beta \Rightarrow \gamma \mid \beta_1$. Siispä $\text{syt}(\alpha, \beta) = \beta_1$. Oletetaan, että $\beta_2 \neq 0$. Nyt on olemassa sellaiset γ_3, $\beta_3 \in O$, että

$$\beta_1 = \gamma_3\beta_2 + \beta_3 \quad \text{ja} \quad |\mathbf{N}(\beta_2)| < |\mathbf{N}(\beta_3)|.$$

Jatketaan tätä menetelmää, kunnes löydetään $\beta_n = 0$. Nyt ollaan saatu kokonaislukujen jono β, β_1,..., missä

$$|\mathbf{N}(\beta)| > |\mathbf{N}(\beta_1)| > |\mathbf{N}(\beta_2)| > \dots.$$

Luvut $|\mathbf{N}(\beta_j)| \in \{1, 2, \dots\}$ muodostavat äärellisen laskevan jonon. Voidaan olettaa, että jonon viimeinen alkio on β_n. Siis

$$\begin{aligned}
\alpha &= \gamma_1\beta + \beta_1 \\
\beta &= \gamma_2\beta_1 + \beta_2 \\
\beta_1 &= \gamma_3\beta_2 + \beta_3 \\
&\vdots \\
\beta_{n-4} &= \gamma_{n-2}\beta_{n-3} + \beta_{n-2} \\
\beta_{n-3} &= \gamma_{n-1}\beta_{n-2} + \beta_{n-1} \\
\beta_{n-2} &= \gamma_n\beta_{n-1} + 0.
\end{aligned}$$

Viimeisen yhtälön perusteella $\beta_{n-1} \mid \beta_{n-2}$, sitä edellisen perusteella $\beta_{n-1} \mid \beta_{n-3}$ aina ensimmäisiin yhtälöihin asti, eli $\beta_{n-1} \mid \beta$ ja $\beta_{n-1} \mid \alpha$. Siis määritelmän 4.3 kohta 1) on voimassa.

Nyt

$$\begin{aligned}
\beta_{n-1} &= \beta_{n-3} - \gamma_{n-1}\beta_{n-2} \\
&= \beta_{n-3} - \gamma_{n-1}(\beta_{n-4} - \gamma_{n-2}\beta_{n-3}) \\
&= -\gamma_{n-1}\beta_{n-4} + (1 + \gamma_{n-1}\gamma_{n-2})\beta_{n-3} \\
&\vdots \\
&= \alpha\zeta + \beta\eta,
\end{aligned}$$

joillakin $\zeta, \eta \in O$. Siispä jokainen kokonaisluku, joka jakaa luvut α, β, jakaa myös luvun β_{n-1}. Siis määritelmän 4.3 kohta 2) on voimassa.

Yksikäsitteisyys: Jokainen luvun $\delta = \text{syt}(\alpha, \beta)$ liitännäisluku toteuttaa suurimman yhteisen tekijän ehdot. Kääntäen, oletetaan, että myös luku $\delta' = \text{syt}(\alpha, \beta)$. Koska $\delta \mid \alpha$, $\delta \mid \beta$ ja $\delta' = \text{syt}(\alpha, \beta)$, niin $\delta \mid \delta'$. Vastaavasti, koska $\delta' \mid \alpha$, $\delta' \mid \beta$ ja $\delta = \text{syt}(\alpha, \beta)$, niin $\delta' \mid \delta$. Lauseen 3.6 nojalla δ' ja δ ovat liitännäisiä.

Todistetaan vielä lauseen viimeinen väite. Edellisten kohtien nojalla voidaan olettaa, että on olemassa sellainen luku δ, että $\delta = \text{syt}(\alpha, \beta)$ ja δ on luvun β_{n-1} liitännäisluku. Edellä nähtiin, että

$$\beta_{n-1} = \alpha\zeta + \beta\eta,$$

joten on olemassa sellainen yksikkö ε, että

$$\delta = \varepsilon\beta_{n-1} = \alpha(\varepsilon\zeta) + \beta(\varepsilon\eta).$$

□

Lause 4.5. *Jos O on Eukleideen alue, niin se on faktoriaalinen rengas.*

Todistus. (vrt. [4, s. 292]) Oletetaan, että O on Eukleideen alue ja $\pi \mid \alpha\beta$, missä π on alkuluku ja $\alpha, \beta \in O$. Näytetään, että joko $\pi \mid \alpha$ tai $\pi \mid \beta$. Oletetaan, että $\pi \nmid \alpha$, joten myöskään mikään luvun π liitännäisluku ei jaa lukua α. Luvun π tekijät ovat joko liitännäisiä luvun π kanssa tai yksiköitä. Nythän $\pi \nmid \alpha$, joten lukujen

α ja π yhteiset tekijät ovat yksiköitä. Koska jokainen yksikkö jakaa luvun 1, niin syt$(\alpha, \pi) = 1$. Lauseen 4.4 nojalla on olemassa sellaiset $\zeta, \eta \in O$, että

$$\alpha\zeta + \pi\eta = 1,$$

joten

$$(\alpha\beta)\zeta + \pi\beta\eta = \beta.$$

Koska $\pi \mid (\alpha\beta)$, niin $\pi \mid (\alpha\beta\zeta + \pi\beta\eta)$. Siispä $\pi \mid \beta$. Täten lauseen 4.1 nojalla O on faktoriaalinen rengas. □

Lause 4.6. *Joukko* $\mathbb{Q}(\sqrt{d})$ *on Eukleideen kunta, jos* $d \in \{-11, -7, -3, -2, -1, 2, 3, 5\}$.

Todistus. (vrt. [4, s. 293]) Jaetaan todistus osiin seuraavasti:

1) Oletetaan, että $d \not\equiv 1 \pmod 4$, eli $d \in \{-2, -1, 2, 3\}$.

2) Oletetaan, että $d \equiv 1 \pmod 4$, eli $d \in \{-11, -7, -3, 5\}$.

1) Olkoot $\alpha, \beta \in O$ ja olkoon $\beta \neq 0$. Merkitään $\alpha/\beta = x + y\sqrt{d}$, missä $x, y \in \mathbb{Q}$. Jokainen rationaaliluku on kahden kokonaisluvun välissä, ja aina korkeintaan etäisyyden $\frac{1}{2}$ päässä lähimmästä kokonaisluvusta, joten on olemassa sellaiset $r, s \in \mathbb{Z}$, että $|x - r| \leq \frac{1}{2}$, $|y - s| \leq \frac{1}{2}$. Olkoot

$$\gamma = r + s\sqrt{d}, \quad \delta = \beta\left[(x - r) + (y - s)\sqrt{d}\right] = \alpha - \gamma\beta.$$

Nyt

$$\begin{aligned} \alpha &= \beta(x + y\sqrt{d}) \\ &= \beta\gamma + \delta. \end{aligned}$$

Koska $r, s \in \mathbb{Z}$, niin $\gamma \in O$, ja koska $\delta = \alpha - \beta\gamma$, niin $\delta \in O$. Tällöin

$$\begin{aligned} |\mathbf{N}(\delta)| &= \left|\mathbf{N}(\beta\left[(x - r) + (y - s)\sqrt{d}\right])\right| \\ &= |\mathbf{N}(\beta)| \cdot \left|\mathbf{N}\left[(x - r) + (y - s)\sqrt{d}\right]\right| \\ &= |\mathbf{N}(\beta)| \cdot \left|\left[(x - r)^2 - d(y - s)^2)\right]\right|, \end{aligned}$$

missä kolmioepäyhtälön nojalla

$$\left|\left[(x - r)^2 - d(y - s)^2\right]\right| \leq |x - r|^2 + |-d||y - s|^2 \leq \left(\frac{1}{2}\right)^2 + 3 \cdot \left(\frac{1}{2}\right)^2 = 1.$$

Jotta yhtäsuuruudet olisivat voimassa, niin pitäisi olla $|x-r| = |y-s| = \frac{1}{2}$ ja $d = 3$, mutta tällöinkin

$$\begin{aligned}\left|\left[(x-r)^2 - d(y-s^2)\right]\right| &= \left|\frac{1}{4} - 3 \cdot \frac{1}{4}\right| \\ &= \frac{1}{2} \\ &< 1.\end{aligned}$$

Siis

$$|\mathbf{N}(\delta)| = |\mathbf{N}(\beta)| \cdot \left|\left[(x-r)^2 - d(y-s^2)\right]\right| < \mathbf{N}(\beta) \cdot 1 = \mathbf{N}(\beta),$$

joten $\mathbb{Q}(\sqrt{d})$ on Eukleideen kunta.

2) Olkoot $\alpha, \beta \in \mathcal{O}$, ja $\beta \neq 0$. Asetetaan $\alpha/\beta = x + y\sqrt{d}$, missä $x, y \in \mathbb{Q}$. Luku $2y$ on kahden perättäisen rationaalikokonaisluvun välissä tai $2y \in \mathbb{Z}$, ja lähin kokonaisluku on korkeintaan etäisyyden $\frac{1}{2}$ päässä, joten on olemassa sellainen $s \in \mathbb{Z}$, että $|2y - s| \leq \frac{1}{2}$. Nyt

$$\left|y - \frac{s}{2}\right| \leq \frac{1}{4}.$$

Vastaavasti on olemassa $r \in \mathbb{Z}$, joka on korkeintaan etäisyyden $\frac{1}{2}$ päässä luvusta $x - \left(\frac{s}{2}\right)$, joten

$$\left|\left(x - \frac{s}{2}\right) - r\right| \leq \frac{1}{2}.$$

Olkoon $\gamma = r + s\left[(1+\sqrt{d})/2\right]$, joka on kokonaisluku seurauksen 2.1 perusteella, ja olkoon $\delta = \beta\left[(x - r - \frac{s}{2}) + (y - \frac{s}{2})\sqrt{d}\right] = \alpha - \beta\gamma \in \mathcal{O}$. Nyt

$$\begin{aligned}\alpha &= \beta(x + y\sqrt{d}) \\ &= \beta\gamma + \delta.\end{aligned}$$

Myös

$$|\mathbf{N}(\delta)| = |\mathbf{N}(\beta)| \left|\left(x - r - \frac{s}{2}\right)^2 - d\left(y - \frac{s}{2}\right)^2\right|,$$

missä kolmioepäyhtälön nojalla

$$\begin{aligned}\left|\left(x - r - \frac{s}{2}\right)^2 - d\left(y - \frac{s}{2}\right)^2\right| &\leq \left|x - r - \frac{s}{2}\right|^2 + |d| \cdot \left|y - \frac{s}{2}\right|^2 \\ &\leq \left(\frac{1}{2}\right)^2 + 11\left(\frac{1}{4}\right)^2 \\ &< 1.\end{aligned}$$

Siis

$$|\mathbf{N}(\delta)| < |\mathbf{N}(\beta)|,$$

joten joukko $\mathbb{Q}(\sqrt{d})$ on Eukleideen kunta. □

Kaikki neliökunnat, jotka ovat Eukleideen kuntia ovat tiedossa:

Lause 4.7. *$\mathbb{Q}(\sqrt{d})$ on Eukleideen kunta, jos ja vain jos*
$d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$.

Todistus. (ks. [4, s. 294]) Sivuutetaan. □

Niiden neliökuntien $\mathbb{Q}(\sqrt{d})$, missä O on faktoriaalinen rengas, etsiminen on avoin ongelma. Kompleksisten neliökuntien tapauksessa oneglma on ratkaistu:

Lause 4.8. *Olkoon $d < 0$. Joukko O on faktoriaalinen rengas, jos ja vain jos $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$.*

Todistus. (ks. [4, s. 295]) Sivuutetaan □

Seuraavassa lauseessa esitellään faktoriaaliset renkaat tapauksessa $0 \leq d \leq 100$:

Lause 4.9. *Olkoon $2 \leq d \leq 100$. Tällöin on olemassa tasan 38 reaalineliökuntaa $\mathbb{Q}(\sqrt{d})$, jotka ovat faktoriaalisia renkaita. Nämä saadaan, kun*

$$\begin{aligned} d \in \{&2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, \\ &38, 41, 43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, \\ &83, 86, 89, 93, 94, 97\}. \end{aligned}$$

Lisäksi, kun $2 \leq d \leq 100$, niin on olemassa täsmälleen 60 reaalineliökuntaa.

Todistus. (ks. [4, s. 296]) Sivuutetaan. □

Huomautus. Vastaavasti kuin joukossa O, joukossa $\mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\right\}$ voidaan määritellä seuraavat käsitteet ja todistaa seuraavat tulokset. Oletetaan, että $\alpha, \beta, \gamma, \delta \in \mathbb{Z}[\sqrt{d}]$.

a) $\alpha + \beta, \alpha - \beta, \alpha\beta \in \mathbb{Z}[\sqrt{d}]$.

b) Oletetaan, että $\alpha \neq 0$. Sanotaan, että luku α *jakaa* luvun β, ja kirjoitetaan $\alpha \mid \beta$, jos on olemassa sellainen $\beta_1 \in \mathbb{Z}[\sqrt{d}]$, että $\beta = \alpha\beta_1$. Tällöin myös $\beta/\alpha \in \mathbb{Z}[\sqrt{d}]$.

c) $|\alpha| \in \mathbb{Z}$.

d) Lukua γ kutsutaan *yksiköksi*, jos $\gamma \mid 1$.

e) Luku γ on yksikkö, jos ja vain jos sen normi on ± 1.

f) Lukua δ kutsutaan *alkuluvuksi* joukossa $\mathbb{Z}[\sqrt{d}]$, jos jokaisessa luvun δ hajotelmassa on $\delta = \delta_1\delta_2$, missä $\delta_1, \delta_2 \in \mathbb{Z}[\sqrt{d}]$, joko δ_1 on yksikkö tai δ_2 on yksikkö.

g) Oletetaan, että $\alpha, \beta \neq 0$. Jos $\alpha = \gamma\beta$, missä γ on yksikkö, niin α ja β ovat *liitännäisiä*.

h) Luvut α ja β ovat liitännäisiä, jos ja vain jos $\alpha \mid \beta$ ja $\beta \mid \alpha$.

i) Joukossa $\mathbb{Z}[\sqrt{d}]$ on äärettömän monta yksikköä, jos $d > 0$.

j) Jokainen ei-yksikkö $0 \neq \alpha \in \mathbb{Z}[\sqrt{d}]$ voidaan esittää äärellisen monen alkuluvun tulona joukossa $\mathbb{Z}[\sqrt{d}]$.

k) Joukko $\mathbb{Z}[\sqrt{d}]$ on *faktoriaalinen rengas*, jos sen tekijähajotelmat ovat samat järjestystä ja liitännäisyyttä vaille.

Lause 4.10. *Jos $\mathbb{Z}[\sqrt{d}]$ on faktoriaalinen rengas, niin luku 2 ei ole alkuluku joukossa $\mathbb{Z}[\sqrt{d}]$.*

Todistus. (ks. [4, s. 297]) Joko d on parillinen tai $d - 1$ on parillinen, joten $2 \mid d(d-1)$. Koska

$$(d + \sqrt{d})(d - \sqrt{d}) = d^2 - d = d(d-1),$$

niin

$$2 \mid (d + \sqrt{d})(d - \sqrt{d}).$$

Mutta $2 \nmid (d + \sqrt{d})$ eikä $2 \nmid (d - \sqrt{d})$ joukossa $\mathbb{Z}[\sqrt{d}]$, koska $(\frac{d}{2} + \frac{1}{2}\sqrt{d})$, $(\frac{d}{2} - \frac{1}{2}\sqrt{d}) \notin \mathbb{Z}[\sqrt{d}]$. Nyt luku 2 jakaa kahden luvun tulon, mutta se ei jaa kumpaakaan

sen tekijää. Lauseen 4.1 nojalla, koska $\mathbb{Z}[\sqrt{d}]$ on faktoriaalinen rengas, niin luku 2 ei ole alkuluku. □

Lause 4.11. *a) Oletetaan, että $d < 0$. Joukko $\mathbb{Z}[\sqrt{d}]$ on faktoriaalinen rengas, jos ja vain jos $d \in \{-2, -1\}$.*

b) Jos $d \equiv 1 \pmod 4$, niin joukko $\mathbb{Z}[\sqrt{d}]$ ei ole faktoriaalinen rengas.

Todistus. (vrt. [4, s. 297]) Osoitetaan, että jos $d \leq -3$ tai $d \equiv 1 \pmod 4$, niin luku 2 on alkuluku joukossa $\mathbb{Z}[\sqrt{d}]$, jolloin lauseen 4.10 nojalla $\mathbb{Z}[\sqrt{d}]$ ei ole faktoriaalinen rengas.

a) Lauseen 4.8 nojalla $\mathbb{Z}[\sqrt{-1}]$ ja $\mathbb{Z}[\sqrt{-2}]$ ovat faktoriaalisia renkaita. Tarkastellaan nyt tapausta $d \leq -3$. Oletetaan, että luku 2 ei ole alkuluku joukossa $\mathbb{Z}[\sqrt{d}]$. Nyt on olemassa sellaiset $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$, että

$$2 = \alpha\beta, \quad |\mathbf{N}(\alpha)| > 1, \quad |\mathbf{N}(\beta)| > 1,$$

joten $\mathbf{N}(\alpha)\mathbf{N}(\beta) = \mathbf{N}(\alpha\beta) = \mathbf{N}(2) = 4$. Koska $|\mathbf{N}(\alpha)|, |\mathbf{N}(\beta)| \in \mathbb{Z}$ ja $|\mathbf{N}(\alpha)| > 1$ ja $|\mathbf{N}(\beta)| > 1$, niin on oltava

$$|\mathbf{N}(\alpha)| = |\mathbf{N}(\beta)| = 2.$$

Merkitään

$$\alpha = a + b\sqrt{d},$$

missä $a, b \in \mathbb{Z}$. Tällöin

$$\begin{aligned} \mathbf{N}(\alpha) &= (a + b\sqrt{d})(a - b\sqrt{d}) \\ &= a^2 - db^2 \\ &= \pm 2. \end{aligned}$$

Jos $b \neq 0$, niin

$$a^2 - db^2 = a^2 + (-d)b^2 \geq 0 + 3 \cdot 1 > \pm 2.$$

Jos $b = 0$, niin

$$a^2 - db^2 = a^2 \neq \pm 2,$$

koska $a \in \mathbb{Z}$. Siis tapauksessa $d \leq -3$ ei ole olemassa sellaista lukua joukossa $\mathbb{Z}[\sqrt{d}]$, jonka normi on ± 2, joten 2 on alkuluku joukossa $\mathbb{Z}[\sqrt{d}]$. Tällöin lauseen 4.10 nojalla $\mathbb{Z}[\sqrt{d}]$ ei ole faktoriaalinen rengas, jos $d \leq -3$.

b) Oletetaan, että luku 2 ei ole alkuluku joukoss $\mathbb{Z}[\sqrt{d}]$ ja $d \equiv 1 \pmod 4$. Tällöin

$$\mathbf{N}(\alpha) = a^2 - b^2 \equiv a^2 - db^2 = \pm 2 \equiv 2 \pmod 4,$$

koska neliöiden jakojäännös $\pmod 4$ on aina 0 tai 1, niin $a^2 - b^2 \equiv \pm 1 \pmod 4$ tai $a^2 - b^2 \equiv 0 \pmod 4$. Siis yhtälöllä

$$a^2 - b^2 \equiv 2 \pmod 4$$

ei ole ratkaisua, missä $a, b \in \mathbb{Z}$. Siispä 2 on alkuluku joukossa $\mathbb{Z}[\sqrt{d}]$, joten lauseen 4.10 nojalla $\mathbb{Z}[\sqrt{d}]$ ei ole faktoriaalinen rengas. □

5 Sovelluksia Diofantoksen yhtälöihin

Lause 5.1. *Diofantoksen yhtälöllä*

$$y^2 + 4 = z^3$$

on vain rationaalikokonaislukuratkaisut $y = \pm 11$, $z = 5$ *ja* $y = \pm 2$, $z = 2$.

Todistus. (vrt. [5, s. 94]) Oletetaan ensin, että $y \in \mathbb{Z}$ on pariton. Polynomi $y^2 + 4$ voidaan jakaa tekijöihin faktoriaalisessa renkaassa $\mathbb{Z}[\sqrt{-1}]$. Tällöin yhtälö saadaan muotoon

$$(2 + iy)(2 - iy) = z^3.$$

Oletetaan, että $a + ib$, missä $a, b \in \mathbb{Z}$, on lukujen $2 + iy$, $2 - iy$ yhteinen tekijä. Tällöin $a + ib$ jakaa näiden lukujen summan ja erotuksen, eli

$$a + ib \mid 4 \quad a + ib \mid 2iy.$$

Normit ottamalla saadaan

$$a^2 + b^2 \mid 16 \quad a^2 + b^2 \mid -4y^2.$$

Koska y on pariton, niin y^2 on pariton. Täten $\text{syt}(16, -4y^2) = 4$, joten määritelmän 4.3 perusteella $a^2 + b^2 \mid 4$. Ainoat mahdolliset arvot ovat

- $a = \pm 1$ ja $b = 0$
- $a = 0$ ja $b = \pm 1$
- $a = \pm 1$ ja $b = \pm 1$
- $a = \pm 2$ ja $b = 0$
- $a = 0$ ja $b = \pm 2$.

Tällöin joko $a + ib$ on yksikkö (kaksi ensimmäistä tapausta) tai $\mathbf{N}(a + ib)$ on parillinen ja $\mathbf{N}(a + ib) \mid \mathbf{N}(2 + iy)$ (loput tapaukset). Koska $\mathbf{N}(2 + iy)$ on pariton, niin jälkimmäinen tapaus ei ole mahdollinen. Täten $\text{syt}(2 + iy, 2 - iy) = 1$.

Lauseen 4.2 perusteella on olemassa sellaiset $\alpha, \beta \in O$ ja sellaiset yksiköt $\varepsilon, \varepsilon'$, että

$$2 + iy = \varepsilon\alpha^3 \quad \text{ja} \quad 2 - iy = \varepsilon'\beta^3.$$

Lauseen 3.4 nojalla joukon $\mathbb{Q}(\sqrt{-1})$ yksiköt ovat ± 1 ja $\pm i$, jotka ovat kuutioita. Siis voidaan olettaa, että $\varepsilon = \varepsilon' = 1$. Merkitään

$$\alpha = a + ib,$$

missä $a, \in \mathbb{Z}$. Tällöin

$$2 + iy = (a + ib)^3,$$

mistä liittoluvut ottamalla saadaan

$$2 - iy = (a - ib)^3.$$

Laskemalla yhteen edelliset yhtälöt, nähdään, että

$$\begin{aligned} 4 &= (a + ib)^3 + (a - ib)^3 \\ &= 2a(a^2 - 3b^2), \end{aligned}$$

joten

$$a(a^2 - 3b^2) = 2.$$

Nyt $a \mid 2$, joten $a = \pm 1$ tai $a = \pm 2$.

- Jos $a = 1$, niin $3b^2 = -1$, mikä on ristiriita.
- Jos $a = -2$, niin $6b^2 = 10$, mikä on ristiriita koska $6 \nmid 10$.
- Jos $a = -1$, niin $b = \pm 1$. Koska $z^3 = ((a + ib)(a - ib))^3 = (a^2 + b^2)^3$, niin oltava $z = a^2 + b^3 = 2$. Tällöin $y^2 + 4 = 8$, joten $y = \pm 2$, mikä on ristiriita, sillä y on pariton.
- Jos $a = 2$, niin $b = \pm 1$ ja $z = a^2 + b^2 = 5$. Tällöin $y^2 + 4 = 125$, joten $y = \pm 11$.

Oletetaan sitten, että y on parillinen, eli $y = 2Y$ jollakin $Y \in \mathbb{Z}$. Täten myös z on parillinen, eli $z = 2Z$ jollakin $Z \in \mathbb{Z}$. Sijoittamalla nämä yhtälöön $y^2 + 4 = 8$ saadaan

$$Y^2 + 1 = 2Z^3,$$

joten luvun Y on oltava pariton. Merkitään $Y = 2k + 1$, missä $k \in \mathbb{Z}$. Tässä $Y^2 + 1 = (Y + i)(Y - i)$. Olkoon α lukujen $Y + i$ ja $Y - i$ yhteinen tekijä. Tällöin

$$\alpha \mid (Y + i) - (Y - i),$$

missä

$$(Y + i) - (Y - i) = 2i = (1 + i)^2.$$

Huomataan, että

$$(Y + i) = (1 + i)\left(\frac{Y + 1}{2} + \left(\frac{1 - Y}{2}\right)i\right) \text{ ja}$$
$$(Y - i) = (1 + i)\left(\frac{Y - 1}{2} - \left(\frac{Y + 1}{2}\right)i\right),$$

missä $\frac{Y+1}{2}, \frac{1-Y}{2}, \frac{Y-1}{2}, \frac{-Y-1}{2} \in \mathbb{Z}$, koska Y on pariton, joten

$$1 + i \mid Y + i \quad \text{ja} \quad 1 + i \mid Y - i.$$

Toisaalta, koska $\alpha \mid (1 + i)^2$ ja $1 + i$ on alkuluku, niin α on yksikkö tai α ja $1 + i$ ovat liitännäisiä tai α ja $(1 + i)^2$ ovat liitännäisiä. Viimeinen tapaus ei ole mahdollinen, koska tällöin olisi

$$\mathbf{N}(\alpha) = \mathbf{N}((1 + i)^2) = 4,$$

mutta

$$\mathbf{N}(Y + i) = 4k^2 + 4k + 2 \equiv 2 \pmod 4,$$

joten

$$\mathbf{N}(\alpha) = 4 \nmid \mathbf{N}(Y + i),$$

mikä on ristiriita. On siis osoitettu, että

$$1 + i = \text{syt}(Y + i, Y - i).$$

Nyt

$$(1 + iY)(1 - iY) = 2Z^3,$$

missä $1 + iY = i(Y - i)$ ja $1 - iY = -i(Y + i)$. Kirjoitetaan

$$Y + i = (1 + i)A \quad \text{ja} \quad Y - i = (1 + i)B,$$

missä $A, B \in \mathcal{O}$. Tällöin syt$(A, B) = 1$ ja $(1+i)^2 AB = 2Z^3$, mistä saadaan ratkaistua $AB = (-i)z^3$. Tällöin lauseen 4.2 nojalla on olemassa sellaiset $a, b \in \mathbb{Z}$, että

$$1 + iY = (1 + i)(a + ib)^3.$$

Liittoluvut ottamalla saadaan

$$1 - iY = (1 - i)(a - ib)^3.$$

Lasketaan yhteen edelliset yhtälöt, jolloin

$$2 = (1 + i)(a + ib)^3 + (1 - i)(a - ib)^3,$$

ja edelleen

$$1 = a^3 - 3ab^2 - 3a^2b + b^3$$
$$1 = (a + b)((a + b)^2 - 6ab).$$

Nyt $a + b = 1$ ja $(a + b)^2 - 6ab = 1$ tai $a + b = -1$ ja $(a + b)^2 - 6ab = -1$, joten oltava $a = 1$ ja $b = 0$ tai $a = 0$ ja $b = 1$. Sijoittamalla nämä aiempiin yhtälöihin saadaan $y = \pm 2$ ja $z = 2$. □

Apulause 5.1. Olkoon p alkuluku. Yhtälöllä

$$x^2 \equiv -1 \pmod{p}$$

on ratkaisu, jos $p = 2$ tai $p \equiv 1 \pmod 4$. Jos $p \equiv 3 \pmod 4$, niin yhtälöllä ei ole olemassa ratkaisua.

Todistus. (ks. [4, s. 103]) Sivuutetaan. □

Apulause 5.2. Olkoon p alkuluku ja $p \equiv 3 \pmod 4$. Jos on olemassa sellaiset a, $b \in \mathbb{Z}$, että

$$a^2 + b^2 \equiv 0 \pmod p,$$

niin

$$a \equiv b \equiv 0 \pmod p.$$

Todistus. (ks. [4, s. 104]) Sivuutetaan. □

Lause 5.2. *Olkoon p rationaalialkuluku.*

a) Jos $p \equiv 3 \pmod 4$, *niin p on alkuluku joukossa* $\mathbb{Q}(\sqrt{-1})$.

b) Jos $p = 2$ *tai* $p \equiv 1 \pmod 4$, *niin p ei ole alkuluku joukossa* $\mathbb{Q}(\sqrt{-1})$. *Itse asiassa joukossa* $\mathbb{Q}(\sqrt{-1})$ *on sellainen alkuluku* π, *että* $\boldsymbol{N}(\pi) = p$.

c) Jos π *on alkuluku joukossa* $\mathbb{Q}(\sqrt{-1})$, *niin jokin seuraavista ehdoista pätee:*

- π *on rationaalialkuluvun* $\pi' \equiv 3 \pmod 4$ *liittoluku.*
- $\boldsymbol{N}(\pi)$ *on rationaalialkuluku ja* $\boldsymbol{N}(\pi) = 1 \pmod 4$.
- $\boldsymbol{N}(\pi) = 2$.

Todistus. (vrt. [4, s. 301]) a) Oletetaan, että $p \equiv 3 \pmod 4$ ja p ei ole alkuluku joukossa $\mathbb{Q}(\sqrt{-1})$. Nyt $p = \alpha\beta$, missä α, $\beta \in \mathcal{O}$ eivät ole yksiköitä, joten

$$\mathbf{N}(\alpha)\mathbf{N}(\beta) = \mathbf{N}(\alpha\beta) = \mathbf{N}(p) = p^2.$$

Koska normit ovat ei-negatiivisia joukossa $\mathbb{Q}(\sqrt{-1})$ ja $\mathbf{N}(\alpha)$, $\mathbf{N}(\beta) > 1$, niin

$$\mathbf{N}(\alpha) = \mathbf{N}(\beta) = p.$$

Nyt $\alpha = a + bi$, missä a, $b \in \mathbb{Z}$, joten

$$p = \mathbf{N}(\alpha) = (a + bi)(a - bi) = a^2 + b^2.$$

Siis

$$a^2 + b^2 \equiv 0 \pmod p.$$

Apulauseen 5.2 nojalla $a \equiv b \equiv 0 \pmod{p}$, eli $p \mid a$, $p \mid b$. Näin ollen $p^2 \mid (a^2+b^2)$. Tämä on mahdotonta, koska $p = a^2 + b^2$. Siis luvun p on oltava alkuluku joukossa $\mathbb{Q}(\sqrt{-1})$.

b) Oletetaan, että $p = 2$. Nyt

$$\mathbf{N}(1 + i) = (1 + i)(1 - i) = 1 - i^2 = 2.$$

Lauseen 3.5 nojalla $(1 + i)$ on alkuluku joukossa $\mathbb{Q}(\sqrt{-1})$. Oletetaan seuraavaksi, että $p \equiv 1 \pmod{4}$. Nyt apulauseen 5.1 mukaan on olemassa sellainen $a \in \mathbb{Z}$, että

$$a^2 + 1 \equiv 0 \pmod{p}.$$

Siis on olemassa sellainen kokonaisluku b, että

$$a^2 + 1 = pb,$$

eli

$$(a + i)(a - i) = pb.$$

Jos p on alkuluku, niin joko $p \mid (a+i)$ tai $p \mid (a-i)$, koska $\mathbb{Z}[\sqrt{-1}]$ on faktoriaalinen rengas. Tämä ei kuitenkaan ole mahdollista, koska $(a/p) + (1/p)i$ ja $(a/p) - (1/p)i$ eivät ole kokonaislukuja. Siis p ei ole alkuluku joukossa $\mathbb{Q}(\sqrt{-1})$. Nyt on olemassa sellaiset kokonaisluvut π_1 ja π_2, jotka eivät ole yksiköitä, ja joille pätee $\pi_1\pi_2 = p$. Tällöin

$$\mathbf{N}(\pi_1)\mathbf{N}(\pi_2) = \mathbf{N}(\pi_1\pi_2) = \mathbf{N}(p) = p^2.$$

Koska $\mathbf{N}(\pi_1)$, $\mathbf{N}(\pi_2) > 1$, niin on oltava

$$\mathbf{N}(\pi_1) = \mathbf{N}(\pi_2) = p.$$

Siispä lauseen 3.5 perusteella sekä π_1 että π_2 ovat alkulukuja joukossa $\mathbb{Q}(\sqrt{-1})$.

c) Olkoon π alkuluku joukossa $\mathbb{Q}(\sqrt{-1})$. Nyt $\mathbf{N}(\pi) \in \mathbb{Z}_+$ ja $\mathbf{N}(\pi) > 1$, joten on olemassa rationaalialkulukujen tulo

$$p_1p_2 \cdots p_n = \mathbf{N}(\pi) = \pi\bar{\pi},$$

missä $p_1, p_2, \ldots, p_n$ ovat rationaalialkulukuja. Koska $\pi \mid p_1p_2 \cdots p_n$, ja $\mathbb{Z}[\sqrt{-1}]$ on faktoriaalinen rengas, niin $\pi \mid p_j$, jollakin $j \in \{1, \ldots, n\}$.

Jos $p_j \equiv 3 \pmod 4$, niin a) kohdan nojalla p_j on alkuluku joukossa $\mathbb{Q}(\sqrt{-1})$, ja siten p_j/π on yksikkö, joten p_j on liitännäinen luvun π kanssa. Oletetaan sitten, että $p_j \not\equiv 3 \pmod 4$ eli $p_j = 2$ tai $p_j \equiv 1 \pmod 4$. Tällöin kohdan b) nojalla p_j ei ole alkuluku. Koska $\pi \mid p_j$, niin on olemassa sellainen $\pi' \in \mathbb{Q}(\sqrt{-1})$, että

$$p_j = \pi\pi'.$$

Täten

$$p_j^2 = \mathbf{N}(p_j) = \mathbf{N}(\pi\pi') = \mathbf{N}(\pi)\mathbf{N}(\pi').$$

Tässä $\mathbf{N}(\pi) \neq 1$, koska π ei ole yksikkö. Jos $\mathbf{N}(\pi') = 1$, niin π' on yksikkö, jolloin π ja p_j ovat liitännäisiä, mistä seuraisi, että p_j olisi alkuluku. Siis oltava $\mathbf{N}(\pi) = \mathbf{N}(\pi') = p_j$. □

Lause 5.3. *Olkoon $n > 0$ rationaalikokonaisluku. Diofantoksen yhtälöllä $x^2+y^2 = n$ on rationaalikokonaislukuratkaisu, jos ja vain jos n voidaan kirjoittaa muodossa $n = m^2k$, missä m, $k \in \mathbb{Z}_+$ ja luvulla k ei ole rationaalialkulukutekijöitä, jotka ovat muotoa $p \equiv 3 \pmod 4$.*

Todistus. (vrt. [4, s. 303]) Oletetaan, että $n = m^2k$, missä m, $k \in \mathbb{Z}_+$ ja, jos $p > 0$ on rationaalialkuluku, joka jakaa luvun k, niin $p \not\equiv 3 \pmod 4$. Jos $k = 1$, niin $n = m^2 + 0^2$. Jos $k > 1$, niin voidaan kirjoittaa

$$k = p_1p_2 \cdots p_r,$$

missä jokainen $p_j = 2$ tai $p_j \equiv 1 \pmod 4$. Lauseen 5.2 nojalla on olemassa sellaiset alkuluvut $\pi_1, \pi_2, \ldots, \pi_r$ joukossa $\mathbb{Q}(\sqrt{-1})$, että

$$\mathbf{N}(\pi_j) = p_j,$$

aina kun $1 \leq j \leq r$. Merkitään

$$a + bi = m\pi_1\pi_2 \cdots \pi_r,$$

missä a, $b \in \mathbb{Z}$. Nyt

$$\begin{aligned} a^2 + b^2 &= \mathbf{N}(a + bi) \\ &= \mathbf{N}(m)\mathbf{N}(\pi_1)\mathbf{N}(\pi_2) \cdots \mathbf{N}(\pi_r) \\ &= m^2 p_1 p_2 \cdots p_r \\ &= m^2 k \\ &= n, \end{aligned}$$

joten on löydetty ratkaisu yhtälölle $x^2 + y^2 = n$.

Kääntäen, oletetaan, että on olemassa sellaiset $a, b \in \mathbb{Z}$, että $a^2 + b^2 = n$. Tällöin

$$\mathbf{N}(a + bi) = n.$$

Jos $a + bi$ on yksikkö joukossa $\mathbb{Q}(\sqrt{-1})$, niin $n = 1$, joka voidaan asettaa haluttuun muotoon $1^2 \cdot 1$. Jos $a + bi$ ei ole yksikkö, niin se voidaan lauseen 3.7 nojalla kirjoittaa alkulukujen tulona joukossa $\mathbb{Q}(\sqrt{-1})$ muodossa

$$a + bi = \pi_1 \pi_2 \cdots \pi_r.$$

Lauseen 5.2 nojalla voidaan olettaa, että $\pi_1, \pi_2, \ldots, \pi_s$ ovat liitännäisiä rationaalialkulukujen $p_1, p_2, \ldots, p_s \equiv 3 \pmod 4$ kanssa, ja luvuilla $\pi_{s+1}, \pi_{s+2}, \ldots, \pi_r$ on normit $p_{s+1}, p_{s+2}, \ldots, p_r$, jotka ovat rationaalialkulukuja ja $p_j = 2$ tai $p_j \equiv 1 \pmod 4$, aina kun $s + 1 \leq j \leq r$. Olkoon

$$m = p_1 p_2 \cdots p_s, \quad k = p_{s+1} p_{s+2} \cdots p_r.$$

Nyt, koska liitännäisten lukujen normit ovat samoja, niin

$$\begin{aligned} n &= \mathbf{N}(a + bi) \\ &= \mathbf{N}(\pi_1)\mathbf{N}(\pi_2) \cdots \mathbf{N}(\pi_s)\mathbf{N}(\pi_{s+1})\mathbf{N}(\pi_{s+2}) \cdots \mathbf{N}(\pi_r) \\ &= \mathbf{N}(p_1)\mathbf{N}(p_2) \cdots \mathbf{N}(p_s)\mathbf{N}(\pi_{s+1})\mathbf{N}(\pi_{s+2}) \cdots \mathbf{N}(\pi_r) \\ &= p_1^2 p_2^2 \cdots p_s^2 p_{s+1} p_{s+2} \cdots p_r \\ &= m^2 k. \end{aligned}$$

Tässä luvun k alkulukutekijät ovat selvästi haluttua muotoa. □

Seuraus 5.1. (vrt. [4, s. 304]) Rationaalialkuluku p voidaan kirjoittaa kahden neliön summana, jos ja vain jos $p \equiv 3 \pmod 4$.

Todistus. Lauseen 5.3 nojalla on olemassa sellainen $a, b \in \mathbb{Z}$, että $p = a^2 + b^2$, jos ja vain jos $p = m^2 k$, missä $m, k \in \mathbb{Z}_+$ ja luvulla k ei ole rationaalilalkulukutekijöitä, jotka ovat muotoa $p \equiv 3 \pmod 4$. Koska p on rationaalialkuluku, niin tällöin on oltava $m = 1$, jolloin $p = k$. Tietenkin luvun p ainoa rationaalialkulukutekijä on p. □

Lähteet

[1] Conrad, Keith, *Factoring in Quadratic Fields*, 2014. http://bit.ly/2eKAfnH, haettu 01.11.2016.

[2] Cook, John D, *Roots of Integers*, 2009. http://bit.ly/2g2sqYe, haettu 01.11.2016.

[3] Milne, J.S, *Algebraic Number Theory*, 2008. http://bit.ly/2flieIJ, haettu 01.11.2016.

[4] Stark, Harold M. *An Introduction to Number Theory*. Tenth printing, MIT Press, Cambridge, Massachusetts and London, England, 1998.

[5] Stewart, I., Tall, D. *Algebraic Number Theory and Fermat's Last Theorem*. Third Edition, AK Peters, Natick, Massachusetts, 2002.

[6] Väisälä, K. *Lukuteorian ja korkeamman algebran alkeet*. Kustannusosakeyhtiö Otava, Helsinki, 1950.

[7] Wikipedia, *Quadratic Integer*. http://bit.ly/2f8zGTk, haettu 16.11.2016.

[8] Wikipedia, *Elements of Euclidean Domain have Greatest Common Divisor*. http://bit.ly/2fZ4hQM, haettu 16.11.2016.